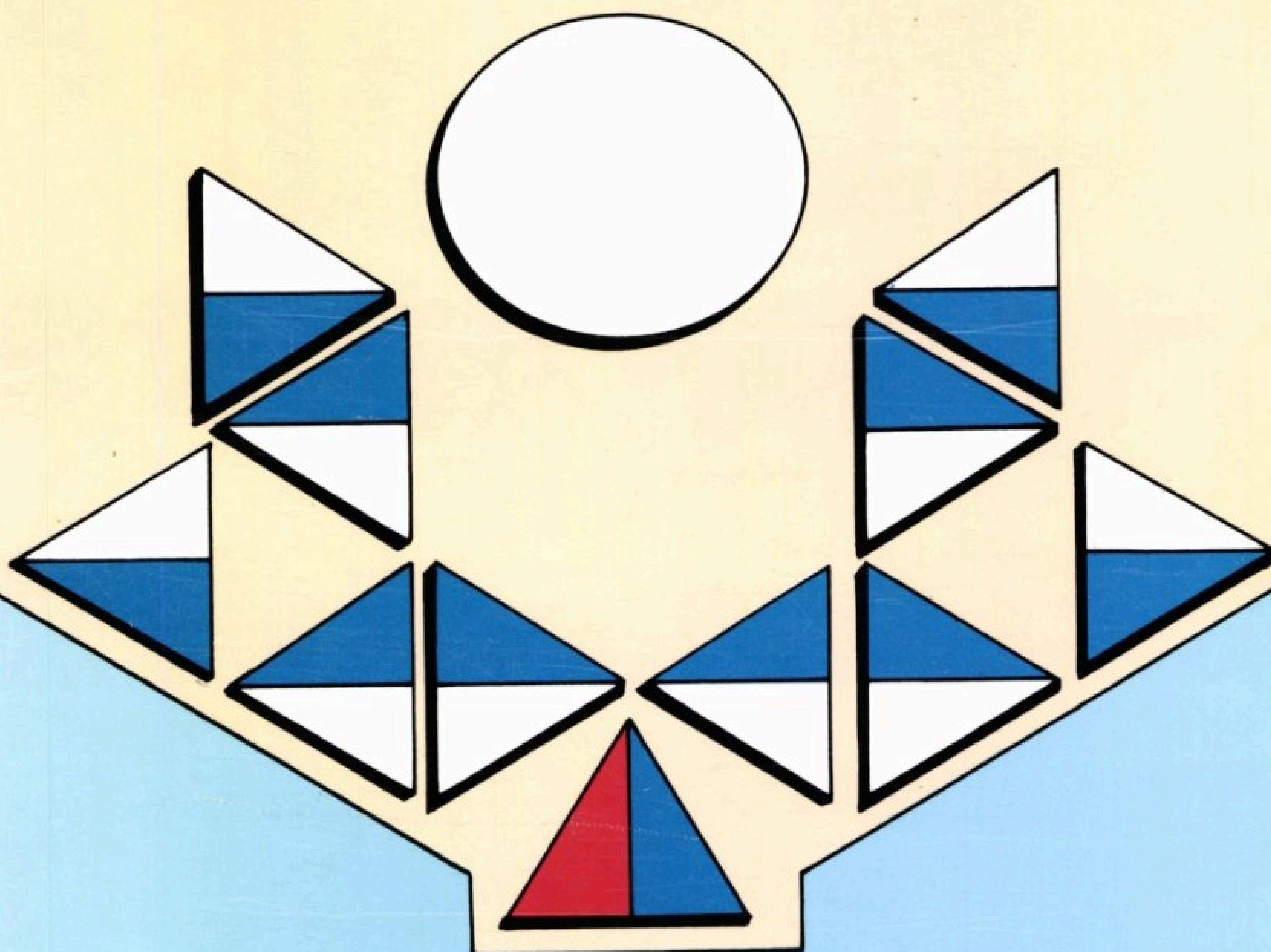
مواضيع في الجبر



تأليف

أي. إن. هيرستين

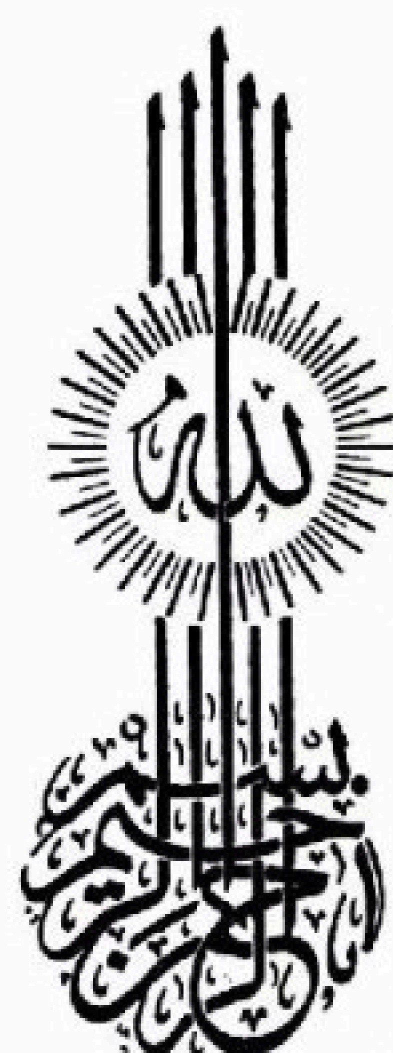
ترجمة

الدكتور فوزي بن أحمد الذكير

الدكتور علي بن عبدالله السحيباني

جامعة الملك سعود

النشر العلمي و المطابع



مواضيع في الجبر

تأليف

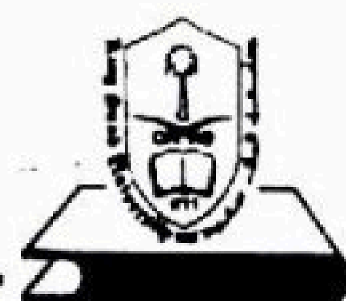
أي. إن. هيريستين

ترجمة

الدكتور فوزي أحمد الذكير
استاذ مشارك

الدكتور علي بن عبدالله السحيباني
استاذ مشارك

قسم الرياضيات، كلية العلوم، جامعة الملك سعود



النشر العلمي والمطابع - جامعة الملك سعود

ص.ب ٢٤٥٤ - الرياض ١١٤٥١ - المملكة العربية السعودية

الطبعة الأولى: ١٤١٤هـ (١٩٩٤م)

الطبعة الثانية: ١٤٢٠هـ (٢٠٠٠م)

الترجمة العربية للطبعة الثانية، مصرح بها لكتاب:

Topics in Algebra, 2nd Edition 1975, by I. N. Herstein.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

هيريستين، أي. إن.

مواضيع في الجبر/ ترجمة فوزي أحمد الذكير، علي عبد الله السحيباني ـــ ط٢. الرياض.

ص ١٧ × ٢٤سم

١- الجبـــر أ- الذكير، فوزي أحمد (مترجم)

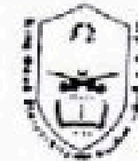
ب- السحيباني علي عبد الله (مترجم) ج- العنوان

ديوي٥١٢ ٢١/٠٠١٤

رقم الإيداع : ٢١/٠٠١٤

ردمك : ٠ - ٨٦ - ٣٧- ٩٩٦٠

تم تحكيم الكتاب بواسطة لجنة متخصصة بناء على قرار المجلس العلمي في اجتماعه الثالث عشر للعام الدراسي ١٤٠٦/١٤٠٧هـ المعقود في ١٧/٦/١٤٠٧هـ الموافق ١٥/٢/١٩٨٧م. ثم وافق المجلس العلمي على إعادة طباعته في تاريخ ٢٠/١١/١٤٢٠هـ الموافق ٢٦/٢/٢٠٠٠م.



النشر العلمي والمطابع ١٤٢١هـ

مقدمة المترجمين

مما لاشك فيه أن حاجة مكتبتنا العربية إلى الكتب العلمية القيّمة أمر يزداد بمرور الزمن وذلك لازدياد عدد الكتب المطبوعة عالميا بشكل هائل. إن أحد الروافد الرئيسة في إثراء مكتبتنا هي الترجمة التي كانت إحدى دعائم الحضارة الإسلامية في عصورها الزاهرة. فلقد ترجم العرب والمسلمون من لغات مختلفة منها اليونانية والهندية والفارسية، وكان لهذه الترجمة الأثر البالغ في نقل ما توصلت إليه تلك الحضارات إلى متناول يد القارىء العربي.

إن ازدياد عدد العرب المتحدثين باللغات الأجنبية لا يُنْقِصُ من أهمية الترجمة إطلاقا، فلقد وجدنا من واقع خبرتنا في التدريس أن معرفة الطالب باللغة الإنجليزية ليست كافية لإعطاءه الشعور بالارتياح في تتبع محتوى كتاب مقرر بتلك اللغة. إن واقع الشعوب المتقدمة دليل على ذلك، فهناك عدد هائل من الكتب الإنجليزية مترجم إلى اللغات الروسية واليابانية والصينية وغيرها، وبالعكس، بالرغم من توفر القرّاء في اللغات المترجم منها.

إن أسباب اختيارنا لهذا الكتاب «**مواضيع في الجبر**» للترجمة تعود إلى ما يلي:

- إن الكتاب يُعَدُّ من الكتب المعتمدة في تدريس مادة الجبر في المرحلتين الثالثة والرابعة لمتخصصي الرياضيات في كثير من الجامعات الأمريكية وبعض الجامعات الأوروبية.

- إن الكتـاب جامع لمختلف مواضيع الجبر المجرد التي يحتاجها الطالب في دراسته الجامعية، فالمادة التي يضمها تغطي ما لا يقل عن محتوى ثلاثة مقررات هي الزمر، الجبر الخطي، والحلقات والحقول.
- من خلال خبرتنا في تدريس هذا الكتاب وجدنا أن أسلوبه سهل وميسر للطالب، حيث إنه يقدم المواضيع الرياضية المجردة بصورة تقربها إلى ذهن الطالب بالإضافة إلى توضيح الدوافع التي دعت المؤلف لتقديم تلك المواضيع.
- حاول المؤلف الابتعاد عن الشكليات وكثرة استعمال الرموز المنطقية التي قد تُنَفِّر الطالب من الموضوع.
- يعتبر مؤلف الكتاب I. N. Herstein ممَّن ساهموا بشكل فعَّال في تطوير علم الجبر من خلال أبحاثه العديدة مما انعكس بشكل إيجابي على أسلوب كتابته، هذا بالإضافة إلى خبرة المؤلف الطويلة في التدريس في جامعة شيكاغو بالولايات المتحدة.

والآن نورد بعض الملاحظات حول الترجمة:

- لقد اتّبعنا الرموز الرياضية نفسها الموجودة في الكتاب إلاَّ ما ندر، وخاصة الرمز J الذي استبدلناه بالرمز Z الأكثر شيوعا للدلالة على مجموعة الأعداد الصحيحة.
- فيما يختص بترجمة المصطلحات حاولنا، قدر الإمكان، التمسك بما ورد في قائمة مكتب تنسيق التعريب في الرباط والمنبثقة من المؤتمر الثالث للتعريب عام ١٩٧٧م. كذلك استعنّا بمعجم الرياضيات الذي نشرته مؤسسة الكويت للتقدم العلمي عام ١٩٨٣م. كما اجتهدنا في ترجمة بعض المصطلحات. ولغرض التسهيل على القارىء: قمنا بإعداد قائمة بالمصطلحات وضعناها في نهاية هذا الكتاب.
- لقد لاحظنا وجود بعض الهفوات المطبعية في النسخة الإنجليزية فقمنا بتصحيحها في الترجمة. كما أننا صححّنا أخطاء رياضية مثل التي وردت في برهان تمهيدية (٧-٤-٥).

هذا ونرجو الله العلي القدير أن يجعل في عملنا هذا الفائدة لدارسي الرياضيات وغيرهم من المهتمين في هذا المجال وأن يوفقنا جميعا لخدمة لغة كتابه الكريم.

المترجمان

مقدمة
الطبعة الثانية

لقد واجهتُ عملية مراجعة كتاب «مواضيع في الجبر»، الطبعة الأولى، بشيء من التخوف. ذلك لأنني كنت، على العموم، راضيا عن الطبعة الأولى ولم أرد تغييرا لها. ومع ذلك فهناك بعض التغييرات التي شعرت بوجوب إجرائها، وهي تغييرات لا تؤثر على الأسلوب العام أو المحتوى ولكنها تجعل الكتاب أكثر اكتمالا. إنني أتمنى أن أكون قد حققت هذه الغاية في هذه الطبعة.

إن أكثر التغييرات قد أجريت على فصل نظرية الزمر. فعندما كتبت الطبعة الأولى لم يكن شائعا أن الطلاّب الدارسين للجبر المجرد قد سبق وأن تعرضوا للجبر الخطي، وفي الوقت الحاضر نجد أن العكس هو الصحيح، إذ أن الكثير من الطلاّب، بل ربما غالبيتهم سبق وأن تعلموا شيئا عن المصفوفات من نوع (2×2) في هذه المرحلة. لذا فإنني شعرت بالحرية في استعمال المصفوفات من نوع (2×2) في الأمثلة والمسائل. إن الأجزاء التي تعتمد على بعض المعرفة في الجبر الخطي قد أشير إليها بالرمز # .

في الفصل المتعلق بالزمر توسعت كثيرا في البند الخاص بمبرهنة سيلو (Sylow)، وقمت بإضافة بندين آخرين، أحدهما عن الضرب المباشر والآخر عن بنية الزمر الإبدالية المنتهية.

في المعالجة السابقة لمبرهنة سيلو اقتصرنا على تبيان وجود زمرة سيلو الجزئية. ولقد استعملنا في ذلك برهان فيلانت (Wielandt) . إن ترافق زمر سيلو الجزئية وعددها كان

من ضمن سلسلة من التمارين ولم يكن في صلب الكتاب. أما الآن فإن جميع أجزاء مبرهنة سيلو تَتَضَمَّنُها مادة الشرح في الكتاب. وبالإضافة إلى البرهان السابق لوجود زمرة سيلو الجزئية نقدم برهانين آخرين للشيء ذاته. قد يتهمني البعض بالإفراط في هذه الناحية وقد يكونوا محقين في ذلك. إن حقيقة الأمر هي أن مبرهنة سيلو مهمة وأن كل برهان يعرض ناحية مختلفة في نظرية الزمر، وأكثر من ذلك أنني معجب بمبرهنة سيلو. أما برهان ترافق وعدد زمر سيلو الجزئية فإنه يستخدم المجموعات المشاركة المزدوجة. إن إحدى النتائج الجانبية لهذا العرض هي طريقة لإيجاد زمر سيلو الجزئية في مجموعة كبيرة من زمر التناظر.

في الطبعة الأولى حذفت موضوع الضرب المباشر. وحيث إن المادة سهلة، ومهمة، في الوقت نفسه، فلقد قمت بسد هذه الثغرة في البند الخاص بالضرب المباشر الذي أضفته في هذه الطبعة. وقمت في البند التالي له ببرهان تفريق الزمرة الإبدالية المنتهية إلى ضرب مباشر لزمر دورية وكذلك برهان وحدانية اللامتغيرات المصاحبة لهذا التفريق. في الحقيقة إن هذا التفريق كان ضمن محتويات الطبعة الأولى وفي نهاية فصل فضاءات المتجهات كنتيجة لبناء الفضاءات الحلقية المنتهية التوليد على الحلقات الإقليدية. ومع ذلك فإن حالة الزمرة الإبدالية المنتهية مهمة في حَدِّ ذاتها وهذا ما يؤكده البند الخاص بدراسة هذه الزمر. إن وجود هذا البند في الفصل الخاص بالزمر في بداية الكتاب يزيد من احتمال تدريسه.

إن هناك بندا آخر بكامله أضيف في نهاية فصل نظرية الحقول. لقد رأيت أنه من الواجب أن يرى الطالب كثيرة حدود معيّنة على حقل معينً تكوِّن زمرة جالوا له هي زمرة التناظر من الدرجة الخامسة، وبالتالي فإنه لا يمكن التعبير عن جذور كثيرة الحدود هذه. باستخدام الجذور التربيعية، التكعيبية. . . الخ لعناصر من الحقل. ومن أجل عمل ذلك أثبتنا أولا مبرهنة تعطي معيارًا لكون زمرة جالوا لكثيرة حدود غير مختزلة من الدرجة p على حقل الأعداد النسبية، حيث p عدد أولي، هي الزمرة S_p. وكتطبيق لهذا المعيار نحصل على كثيرة حدود من الدرجة 5 على حقل الأعداد النسبية والتي زمرة جالوا لها هي زمرة التناظر من الدرجة 5 .

هناك العديد من الإضافات الأخرى. فيوجد أكثر من 150 مسألة جديدة تختلف في درجة صعوبتها، بعض هذه المسائل روتينية وحسابية والعديد منها صعب جدًا، وبالإضافة إلى ذلك، فهناك بعض الملاحظات البينية التي وضعت في المسائل التي يواجه فيها القرّاء صعوبة شديدة. لقد أدرجت بعض الفقرات الجديدة بينما أعيد كتابة بعضها الآخر في الأماكن التي كانت فيها العبارات غامضة أو وجيزة.

لقد بيّنت فيما سبق ما قمت بإضافته. أما الذي لم أضفه فقد سبب لي القرار بشأنه صعوبة بالغة. فقد فكّرت كثيرا في إضافة فصل لنظرية الطوائف (الفصائل) وبعض الدلّالات الابتدائية وكذلك التوسع في دراسة الفضاءات الحلقية. وبعد التفكير مليًا في الأمر قررت عدم إضافة شيء من ذلك. إن الكتاب كما هو الآن يحوي مواضيع متماسكة لا تمتزج مع المواضيع الجديدة التي فكّرتُ فيها. إنه من الممكن مزج هذه المواضيع بما هو موجود ولكن ذلك يتطلب إعادة كتابة مادة الكتاب بأكملها وتغييرا كليا لفلسفته ـ وهو شيء لم أرد فعله. إن مجرد إضافة هذه المادة الجديدة كملحق دون تطبيقات وأهداف معروفة يتعارض مع مبدئي الأساسي الذي ينص على أن المادة التي أتعرض لشرحها يجب أن تؤدي بي إلى أهداف معيّنة، ونقاط بارزة ومبرهنات شيّقة، لذا قررت إلغاء المواضيع الإضافية.

لقد كتب لي الكثير من القرّاء حول الطبعة الأولى مشيرين إلى أخطاء مطبعية أو مقدمين بعض الاقتراحات لتحسين الكتاب، لذلك فإني أنتهز هذه المناسبة لأتقدم إليهم بالشكر على مساعدتهم.

مقدمة
الطبعة الأولى

إن الفكرة من وراء هذا الكتاب، والأكثر من ذلك، الرغبة في عمل هذا الكتاب نشأت مباشرة من مقرر درسته في السنة الأكاديمية ١٩٥٩ ـ ١٩٦٠م في جامعة كورنل. ولقد كان أكثر طلّاب الصف يتكونون من طلّاب السنة الثانية المتميزين في الرياضيات في تلك الجامعة. ولقد كانت رغبتي تجربة عرض مادة لهم أكثر من تلك التي تعطى عادة للمستويين الأول والمتقدم.

ولقد كان هدفي من هذا الكتاب، من حيث المستوى وأسلوب العرض أن يكون وسطا بين كتابين تقليديين: أولهما مسح في الجبر الحديث لمؤلفيه بيركهوف وماكلين والآخر الجبر الحديث لمؤلفه فاندرفيردن.

لقد حدث تغير ملحوظ في السنوات الأخيرة في تعليم الرياضيات في الجامعات الأمريكية وكان هذا التغيير ملحوظا في الصفوف العليا في الجامعة وبداية الدراسات العليا. إن المواضيع التي كانت تعتبر قبل سنوات مناسبة للمقررات شبه المتقدمة للدراسات العليا في الجبر أصبحت الآن تدرس في أول المقررات في الجبر المجرَّد. وعلى افتراض أن هذا التغيير سيستمر بشكل مكثف في السنوات القليلة القادمة فإنني قد وضعت في هذا الكتاب، الذي صمم ليكون أول مقدمة في الجبر للطالب، مادة تعتبر حتى الآن متقدمة قليلا لتلك المرحلة من الدراسة.

إنه عادة ما توجد مخاطرة كبيرة عند معالجة أفكار مجردة بصورة مفاجئة وبدون أساس كاف من الأمثلة بحيث تجعلها معقولة وطبيعية. ومن أجل تخفيف هذا، حاولت سلفا تقديم الدوافع والأفكار اللازمة لتلك الأفكار في أوضاع واقعية. إن أحد الدلائل قوة على كفاءة المفهوم المجرد هو ما يفيدنا به ذلك المفهوم وما ينتج في أوضاع مألوفة. ولقد بذلت محاولة في كل فصل، تقريبا، لاظهار أهمية النتائج العامة وذلك بتطبيقها في مسائل خاصة. فعلى سبيل المثال، عرضت في الفصل المتعلق بالحلقات مبرهنة المربعين لفيرما كنتيجة مباشرة لنظرية الحلقات الإقليدية.

ولقد تم اختيار الموضوع المطروح للمناقشة لا لأنه أصبح قياسيا لعرضه عند هذا المستوى ولا لكونه مهما بصورة عامة ولكن بالنظر «لواقعيته» ولهذا السبب قررت حذف مبرهنة جوردان ـ هولدر والتي كان من الممكن تضمينها في النتائج المتعلقة بالزمر، ورغم ذلك، فإنه لتقدير هذه النتيجة في حد ذاتها يتطلب الأمر تصورا كبيراً لنتائج سابقة أو لاحقة كما أنه لكي نرى استخدامها بكفاءة فإن الأمر يتطلب حيودًا كبيرًا عن الموضوع. صحيح، إنه من الممكن دراسة نظرية بُعد فضاء المتجهات كإحدى نتائج تلك المبرهنة، ولكن، ولأول مرة، يبدو محتملا أن هذا منطلق متطرف وغير طبيعي لأمر أساسي جدا. وبالمثل فإنه لا يوجد ذكر لحاصل الضرب الموتر أو الإنشاءات المتعلقة به. إنه ليوجد متسع من الوقت لدى الطالب لدراسة تلك الأفكار المجردة فيما بعد ومن هنا فَلِمَ العجلة بتقديمها الآن في هذا الكتاب؟

بقيت كلمة حول المسائل التي يوجد عدد كبير منها. إن الطالب المتميز جدا هو الذي قد يكون بإمكانه حل المسائل جميعها. إن بعض المسائل ما هو إلَّا تكملة لبرهان معين وَرَدَ أثناء العرض بينما يكون بعضها ليس إلا توضيحا عمليا لبعض النتائج التي وردت في الكتاب كما أن بعض المسائل قد قُدِّم لا لمجرد حلها بقدر ما هو كيفية البدء بحلها. إن قيمة المسألة ليست بمجرد الحصول على حل لها بقدر ما هي في الأفكار والمحاولات الفكرية التي تقود إلى حلها. ولقد ورد بعض المسائل توطئة لمواضيع ستعالج فيما بعد حيث إن الأمل، والسبب من وراء ذلك وهذا، هو وضع الأساس

للنظرية التي ستطوّر فيما بعد كما إنه يجعل من الأفكار والتعاريف والمناقشة أكثر طبيعية عندما تقدم في حينها . هناك مسائل عديدة ستظهر أكثر من مرة كما أن بعض المسائل التي تبدو لي لسبب أو لآخر صعبة نوعا ما قد وضع عليها نجمة (كما قد وضع على بعضها نجمتان) ومع ذلك فإنه لا يوجد هنا اتفاق بين الرياضيين فمنهم من يرى أن المسائل التي يوضع عليها نجمة كان من المفروض ألا يوضع عليها شيء والعكس صحيح .

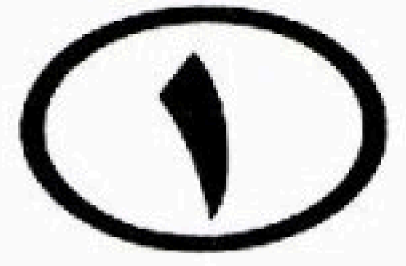
إنني مدين بالشكر لعدد من الأصدقاء وذلك لاقتراحاتهم وتعليقاتهم وانتقاداتهم وأخص بالذكر بعضا منهم شارل كيرتز، مارشال هول، ناثان جاكوبسون، آرثر ماتوك، ماكسويل روزفلخت . كما أنني مدين بالشكر لدانيال جورنشتاين وإيرفنج كابلانسكي وذلك لمناقشاتنا العديدة حول الكتاب من حيث مادته وأفكاره . وقبل كل شيء، أشكر جورج سيلجمان لاقتراحاته الواضحة وملاحظاته حول طريقة العرض والمحتوى كما أنني أشكر فرانسيس مكناري الموظف في شركة جن وشركاه لتعاونه ومساعدته . وأخيرا أود أن أعبر عن شكري لمؤسسة جون سايمون جوجنهايم موموريال لإعانتهم المؤلف في كتابة جزء من هذا الكتاب وذلك عندما كان في روما زميلا لمؤسسة جوجنهايم .

المحتويات

صفحة

صفحة

صفحة



أفكار أولية

● نظرية المجموعات ● التطبيقات
● الأعداد الصحيحة

إن من أحد المعالم المهمة لرياضيات القرن العشرين هو ادراك المشتغلين بها بقوة الطريقة التجريدية وقدكان هذا باعثا مهما لنتائج ومسائل جديدة، ومن ثم، قادنا ذلك إلى استكشاف مجالات جديدة في الرياضيات لم تخطر على بال أحد من قبل.

ولم ينتج عن هذه التطورات رياضيات جديدة فحسب بل نتج عنها أيضا وجهات نظر جديدة، وإلى جانب هذا براهين جديدة وبسيطة لنتائج تقليدية صعبة. إن إعادة مسألة ما إلى أساسياتها تظهر لنا الوضع الصحيح لها، فالنتائج التي كان يعتقد بأنها حالات خاصة منفصلة أصبحت ترتبط مع بعضها البعض من خلال هذه الأساسيات.

ولا يُعتبر موضوع الجبر الذي تطور من خلال هذه المفاهيم هو موضوع مستقل بذاته، بل إنه يربط بين فروع الرياضيات مثل الهندسة، نظرية الأعداد، التحليل والتوبولوجيا وحتى الرياضيات التطبيقية، كما يعتبر أحد مجالات البحث الحديثة المهمة في حقل الرياضيات.

ولقد أُعدَّ هذا الكتاب ليكون مدخلاً لهذا الفرع من الرياضيات الذي يدعى اليوم بالجبر المجرد. إن كلمة «مجرد» هي تعبير ذو صفة شخصية بمعنى أنها تعني عند

إنسان ما شيئا محدداً، بينما تعني شيئا مختلفا عند إنسان آخر. فيما يتعلق بالبحوث الجارية في الجبر يمكن وصف هذا النشاط بأنه ليس تجريديا من وجهة نظر إنسان درس موضوع التفاضل والتكامل، ولكنه يمكن أن يوصف بأنه تجريدي جدا من وجهة نظر إنسان يرى هذه المادة العلمية لأول مرة.

ومهما يكن من أمر، فإننا سنعنى بتقديم بعض الأنظمة الجبرية المهمة وتطورها، مثل الزمر، الحلقات، فضاءات المتجهات، والحقول. ويمكن وصف النظام الجبري بأنه عبارة عن مجموعة من العناصر مزودة بعمليات تمكننا من تركيب هذه العناصر.

وقبل أن نبدأ بدراسة المجموعات من حيث كونها مزودة بعمليات، فإن من الضروري دراستها مجردة عن هذه العمليات ودراسة بعض الأفكار المتعلقة بها. ومن ناحية أخرى، سنحتاج إلى بعض المعلومات عن مجموعة خاصة هي مجموعة الأعداد الصحيحة. إن الغرض من هذا الفصل هو مناقشة موضوع المجموعات ومجموعة الأعداد الصحيحة واشتقاق بعض النتائج التي سنحتاج إليها في مناسبات عديدة من هذا الكتاب.

(١ ـ ١) نظرية المجموعات

لن نحاول إعطاء تعريف معين **للمجموعة** (Set) ولن نمهد لموضوعات نظرية المجموعات، ولكن بدلا من ذلك سنأخذ المنطلق الأوَّلي والعملي، بمعنى أن مجموعة ما هي تجمع من الأشياء. في كثير من تطبيقاتنا سنتعامل مع أشياء محددة، والتي ستتضح من خلالها الفكرة العامة للمجموعة كشيء معقول تماما. وبالنسبة لأولئك الذين يميلون إلى الجانب التجريدي فإننا سنعتبر المجموعة على أنها فكرة أولية لا يمكن تعريفها.

سنبدأ ببعض الملاحظات حول الاصطلاحات والرموز. إذا كان لدينا مجموعة ما ولتكن S ، فإننا سنستخدم الرمز "$a \in S$" ليعني أن "a عنصر من S" . وبالطريقة

نفسها فإن "$a \notin S$" يعني أن "a ليس عنصرا من S" . يقال عن المجموعة A إنها **مجموعة جزئية** (Subset) من S إذا كان كل عنصر من A هو عنصر من S ، أي أنه إذا كان "$a \in A$" فإن هذا يقتضي أن "$a \in S$" ، وسنكتب هذا على الشكل $A \subset S$ [وأحيانا $S \supset A$] والتي يمكن أن تقرأ A محتواة في S [أو S تحتوي على A]. إن هذا الرمز لا يعني استبعاد إمكانية كون A تساوي S .

وبهذه المناسبة، **ماذا نقصد بتساوي مجموعتين؟**
إن هذا يعني بالنسبة لنا أن كُلًّا منهما تحتوي على العناصر نفسها، وبمعنى آخر، إن كل عنصر في إحدى المجموعتين ينتمي إلى الأخرى والعكس صحيح . وبالتعبير عن ذلك بدلالة رمز الاحتواء فإن المجموعتين A و Bتكونان متساويتين ونكتب $A = B$ إذا كانت $A \subset B$ و $B \subset A$. إن الطريقة المثلى لبرهان تساوي مجموعتين والتي سنطلبها أحيانا هي برهان أن علاقتي الاحتواء المتعاكستين محققة لكل من المجموعتين.

يقال عن المجموعة الجزئية A من S إنها **مجموعة جزئية فعلية** (Proper Subset) من S إذا كانت $A \subset S$ ولكن $A \neq S$ (أي أن A لا تساوي S). إن **المجموعة المعدومة** (Null set) هي تلك المجموعة التي لا تحتوي على أي عنصر، وهي مجموعة جزئية في أية مجموعة. وغالبا سنصف مجموعة بأنها معدومة بقولنا إنها **خالية** (Empty) . وأخيرا ملاحظة رمزية بحتة هي أنه إذا كانت S مجموعة فإن الرمز A حيث $A = \{ a \in S \mid P(a)\}$ يعني " مجموعة العناصر من S التي تحقق الخاصة P" .

فعلى سبيل المثال:
إذا كانت S هي مجموعة الأعداد الصحيحة وكانت A مجموعة جزئية من الأعداد الصحيحة الموجبة فإنه يمكننا وصف A على الصيغة $A = \{ a \in S \mid a > 0\}$.
ومثال آخر
هو أنه إذا كانت S هي المجموعة التي تتكون من (1),(2),......,(10) فإنه يمكن وصف المجموعة الجزئية A التي تتكون من (1),(4),(7),(10) على النحو التالي:

$$A=\{(i)\in S | i=3n+1, n=0,1,2,3,\}$$

إذا كان لدينا مجموعتان فإن باستطاعتنا تركيبهما لكي نحصل على مجموعات جديدة. إنه لا يوجد أية خصوصية لاختيار العدد اثنين إذ أنه باستطاعتنا اتخاذ هذا الإجراء لأي عدد من المجموعات، سواء أكان هذا العدد منتهيا أم غير منتهٍ. إن سبب اختيارنا لمجموعتين يعود إلى أنه يوضح لنا البنية العامة دون أن نشغل القارىء بصعوبات ترميزية لا داعي لها.

تعريف

إن اتحاد (Union) المجموعتين A وB ويكتب $A \cup B$ هو مجموعة العناصر x بحيث تنتمي x إلى A أو تنتمي x إلى B ($x \in A$ أو $x \in B$).

بقي أن نعلم استخدام الحرف «أو» في اللغة العامة، فعندما نقول إن شيئا ما أو آخر فإننا نعني أنه واحد منهما وليس كليهما، ولكن الأمر من الناحية الرياضية مختلف تماما وخاصة عندما نتكلم عن نظرية المجموعات، لأنه عندما نقول إن العنصر x ينتمي إلى المجموعة A أو إلى المجموعة B فإننا نعني أن x هو على الأقل أحد عناصر A أو B ومن الممكن أن يكون في كليهما معا.

لنرى الآن بعض الأمثلة على اتحاد مجموعتين.

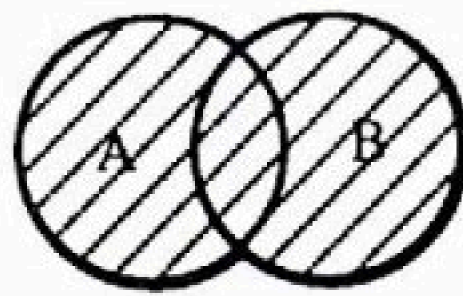
إنه لأية مجموعة A يكون $A \cup A = A$.

وفي الحقيقة، عندما تكون B مجموعة جزئية من A فإن $A \cup B = A$.

وإذا كانت A هي المجموعة $\{x_1, x_2, x_3\}$ [أي أن A هي المجموعة التي عناصرها x_3, x_2, x_1]، وكانت B هي المجموعة $\{y_1, y_2, x_1\}$ فإن:

$$A \cup B = \{x_1, x_2, x_3, y_1, y_2\}$$

وإذا كانت A هي مجموعة الناس ذوي الشعر الأشقر وB هي مجموعة الناس المدخنين فإن $A \cup B$ تتكون من الناس ذوي الشعر الأشقر أو المدخنين أو كليهما وبإمكاننا توضيح اتحاد المجموعتين A و B بالرسم الآتي:



هنا A هي الدائرة التي على اليسار وB هي الدائرة التي على اليمين و$A \cup B$ هو الجزء المظلل.

تعريف

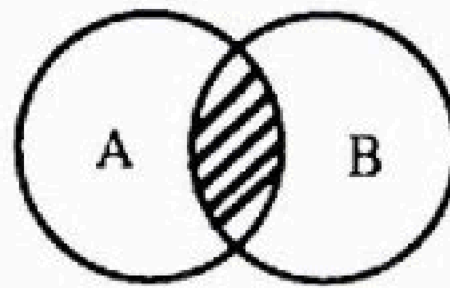
إن تقاطع (Intersection) المجموعتين A وB ويكتب $A \cap B$ هو المجموعة $\{x \mid x \in A, x \in B\}$ وهي مجموعة العناصر التي تنتمي إلى A و B في الوقت نفسه.

سنوضح تقاطع مجموعتين وذلك باستخدام المجموعات التي وردت في توضيح اتحاد مجموعتين.

إنه لأية مجموعة A يكون $A \cap A = A$.

وإذا كانت $A = \{x_1, x_2, x_3\}$ و $B = \{y_1, y_2, x_1\}$ فإن $A \cap B = \{x_1\}$. هذا على افتراض أن $x_i \neq y_j$ حيث $i=1,2,3$ و $j=1,2$.

وإذا كانت A هي مجموعة الناس ذوي الشعر الأشقر وB هي مجموعة الناس المدخنين فإن $A \cap B$ هي مجموعة الناس ذوي الشعر الأشقر والذين يدخنون في الوقت نفسه وبإمكاننا توضيح $A \cap B$ كما في الشكل الآتي:



A هي الدائرة التي على اليسار و B هي الدائرة التي على اليمين و $A \cap B$ هو الجزء المظلل.

يقال عن مجموعتين إنهما منفصلتان إذا كان تقاطعهما خاليا، أي، المجموعة المعدومة، فمثلا، إذا كانت A هي مجموعة الأعداد الموجبة وB هي مجموعة الأعداد السالبة فإن A وB منفصلتان، ومع ذلك، لاحظ أنه إذا كانت C هي مجموعة الأعداد غير السالبة وD هي مجموعة الأعداد غير الموجبة فإن C وD غير منفصلتين لأن تقاطعهما يحتوي على العدد الصحيح «صفر»، وبالتالي فإنه غير خالٍ.

وقبل أن نعمم فكـرة الاتحاد والتقاطع إلى أكثر من مجموعتين سنبرهن قضية صغيرة تربط بين التقاطع والاتحاد. وهذه هي أولى النتائج التي يمكن برهانها، والتي سنترك بقيتها كمسائل عند نهاية هذا البند.

قضيـة

لأي ثلاث مجموعات C,B,A يكون

$$A\cap(B\cup C) = (A\cap B) \cup (A\cap C)$$

البرهان

إن البرهان يتكون من إثبات علاقتي الاحتواء المتعاكستين

$$(A\cap B) \cup (A\cap C) \subset A\cap (B\cup C),$$

$$A\cap (B\cup C) \subset (A\cap B) \cup (A\cap C)$$

سنثبت أولا أن:

$$(A\cap B) \cup (A\cap C) \subset A\cap (B\cup C)$$

لما كان $B \subset (B\cup C)$ فإن من الواضح أن $(A\cap B) \subset A\cap (B\cup C)$
وبطريقة مماثلة نجد أن

$$A\cap C \subset A\cap (B\cup C)$$

ولذلك يكون

$$(A\cap B) \cup (A\cap C) \subset A\cap (B\cup C) \cup A\cap (B\cup C) = A\cap (B\cup C)$$

وبالنسبة للاتجاه الآخر نفرض أن $x \in A\cap(B\cup C)$ عندئذ $x \in A$ و $x \in B \cup C$ ومن ثم فإن $x \in B$ أو $x \in C$.

فلنفـرض أن $x \in B$ ، عنـدئـذ لما كان $x \in A$ و $x \in B$ فإن $x \in A \cap B$. أما إذا كـان $x \in C$ فـإن $x \in A \cap C$ وهـكـذا وفي أيٍّ مـن الاحـتـمـالـين نجـد أن $x \in (A \cap B) \cup (A \cap C)$

ولذلك نجد أن:

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cup C)$$

ومن علاقتي الاحتواء المتعاكستين نحصل على المساواة المطلوبة في القضية.

تستأنف الآن دراسة المجموعات وذلك لتعميم فكرة الاتحاد والتقاطع لأي عدد من المجموعات. ولنفرض أن T مجموعة، نقول إن T هي مجموعة الدليل لعائلة المجموعات $F = \{A_\alpha\}$ إذا كان لأي $\alpha \in T$ يوجد مجموعة A_α في العائلة F . إن مجموعة الدليل قد تكون منتهية أو غير منتهية، وغالبا ما سنأخذ T لتكون مجموعة الأعداد الصحيحة غير السالبة. ومع ذلك، يمكن أن تكون T أي مجموعة غير خالية.

نعني **باتحاد المجموعات** A_α حيث $\alpha \in T$ المجموعة التي تتكون من جميع العناصر x حيث $x \in A_\alpha$ على الأقل لعنصر ما α في T . وسنرمز لهذه المجموعة بالرمز

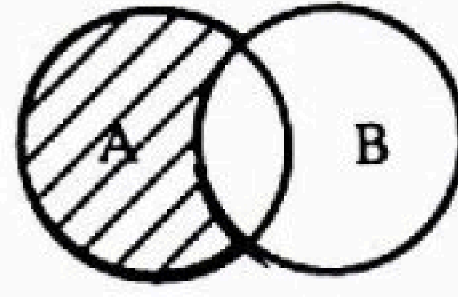
$$\bigcup_{\alpha \in T} A_\alpha$$

كما نعني **بتقاطع المجموعات** A_α حيث $\alpha \in T$ المجموعة التي تتكون من العناصر x حيث $x \in A_\alpha$ لكل $\alpha \in T$ كما سنرمز لهذه المجموعة بالرمز $\bigcap_{\alpha \in T} A_\alpha$.

يقال عن المجموعات A_α إنها **منفصلة تبادليا** (Mutually disjoint) ، إذا كان لكل α و β و $\alpha \neq \beta$ فإن المجموعة $A_\alpha \cap A_\beta$ هي المجموعة المعدومة. فمثلا إذا كانت S هي مجموعة الأعداد الحقيقية وكانت T هي مجموعة الأعداد النسبية وA_α هي المجموعة $\{x \in S | x \geq \alpha\}$ حيث $\alpha \in T$ فإن من السهل إثبات أن $\bigcup_{\alpha \in T} A_\alpha = S$. بينما $\bigcap_{\alpha \in T} A_\alpha$ هي المجموعة المعدومة كذلك فإن المجموعات A_α ليست منفصلة تبادليا [يترك إثبات ذلك كله للقارىء].

تعريف

إذا كانت A و B مجموعتين فإن مجموعة الفرق ***A-B (Difference set)*** *هي المجموعة $\{x \in A / x \notin B\}$ ويمكن أن نمثل A-B بالشكل:*



حيث A هي الدائرة اليسرى وB هي الدائرة اليمنى والجزء المظلل يمثل A-B . ويجب أن نلاحظ أنـــه لأية مجمـــوعـــة B فإن المـــجـــمـــوعـــة A تحقـــق الـــعـــلاقـــة $A=(A\cap B)\cup(A-B)$ [أثبت ذلك]، وزيادة على ذلك فإن $(A-B)\cap B$ هي المجموعة المعدومة.

وحـالـة خاصـة ذات أهمية لمجموعة فرق مجموعتين هي عندما تكون إحدى المجمـوعتـين مجمـوعـة جزئية من الأخرى ففي هذه الحالة عندما تكون $B\subset A$ فإننا نطلق على A-B متممة (Complement) B في A .

نتـــطرق الآن إلى إنشـــاء مجمـوعـة جديدة من المجمـوعتـين A و B . هذه المـجـمـوعـة هي ما يطلق عليهـا الضرب الـديكـارتي (Cartesian Product) للمجمـوعتـين A و B ويرمـز لها بالرمز $A\times B$ ، وتعرف بأنها مجموعة الأزواج المرتبة (a,b) حيث $a\in A$ و $b\in B$. يقـال إن الزوجين (a_1, b_1) ، (a_2, b_2) متساويان إذا وفقط إذا كان $a_1 = a_2$ و $b_1 = b_2$.

ملاحظات على الضرب الديكارتي

- إذا كان لدينا المجموعتان A و B فإنه يمكننا إنشاء المجموعتين $A\times B$ و $B\times A$ منهما. إن هاتين المجموعتين مختلفتان ومع ذلك يمكن للقارىء أن يرى أنهما قريبتا الصلة ببعضهما.
- إذا كان لدينـا المجموعات A و B و C فإننا نستطيع تكوين عدة حواصل ضرب ديكـارتية لها ومنهـا على سبيل المثـال المجموعة $A\times D$ ، حيث $D=B\times C$ والمجموعة $E\times C$ ، حيث $E=A\times B$ ، كذلـك المجمـوعة المكونة من الثلاثيات المرتبة (a,b,c)

حيث $a\in A$ و $b\in B$ و $c\in C$. إننا لانزال نرى تقارب هذه المجموعات الثلاث من بعضها البعض. إننا بالطبع نستطيع الاستمرار بهذه الطريقة لتكوين مجموعات جديدة مع أكثر من ثلاث مجموعات، ولكي نرى العلاقة الوثيقة بين هذه المجموعات علينا أن ننتظر قليلا إلى البند القادم حيث نناقش هناك موضوع التقابلات.

● إذا كان لدينا مجموعة دليل T فإن باستطاعتنا تعريف الضرب الديكارتي للمجموعات A_α حيث α متغير في T . وحيث إننا لن نحتاج إلى هذا الضرب بصورة عامة، لذا فإننا لن نعرفه.

● وأخيرا لنعتبر الضرب الديكارتي للمجموعة A مع نفسها أي $A\times A$. نلاحظ هنا أنه إذا كانت A مجموعة منتهية تحتوي على n من العناصر فإن $A\times A$ مجموعة منتهية تحتوي على n^2 من العناصر.

إن مجموعة العناصر (a,a) في $A\times A$ يطلق عليها **قطر** (Diagonal) $A\times A$.
يقال إن المجموعة الجزئية R من $A\times A$ تُعَرِّفْ **علاقة تكافؤ** (Equivalence relation) على A إذا كان:

١ ـ $(a,a)\in R$ لكل $a\in A$.

٢ ـ $(a,b)\in R$ يقتضي أن $(b,a)\in R$.

٣ ـ إذا كان $(b,c)\in R$ و (a,b) فإن $(a,c)\in R$.

● وعوضا عن التحدث عن مجموعات جزئية من $A\times A$ فإن بإمكاننا التحدث عن علاقة ثنائية على المجموعة A نفسها معرِّفين هذه العلاقة كما يلي: يقال إن للعنصر b علاقة بالعنصر a إذا كان $(a,b)\in R$. إن بالإمكان ترجمة الخواص الثلاث السابقة للمجموعة الجزئية R إلى الخواص الثلاث في التعريف الآتي.

تعريف

يقال إن العلاقة الثنائية ~ على المجموعة A هي علاقة تكافؤ على A إذا تحققت الشروط الآتية لكل a,b,c في A:

١ ـ $a \sim a$

٢ ـ *إذا كان* $a \sim b$ *فإن* $b \sim a$.

٣ ـ *إذا كان* $a \sim b$ *و* $b \sim c$ *فإن* $a \sim c$.

ويطلق على الخاصة الأولى الانعكاسية (Reflexivity) والثانية التناظر (Symmetry) والثالثة التعدي (Transitivity).

إن مفهوم علاقة التكافؤ له أهمية كبرى كما أنه يلعب دورا بارزا في جميع فروع الرياضيات، ولذلك سنوضحه ببعض الأمثلة.

مثال (١ ـ ١ ـ ١)

لنفرض أن S هي أيّة مجموعة، عندئذ نعرف $a \sim b$ لكل a, b في S إذا وفقط إذا كان $a = b$. إن من الواضح أن هذه هي علاقة تكافؤ على S. في الحقيقة إن علاقة التكافؤ هذه ليست إلا تعميما للتساوي وذلك قياسا على خاصة معينة.

مثال (١ ـ ١ ـ ٢)

لنفرض أن S هي مجموعة الأعداد الصحيحة وأن $a, b \in S$ عندئذ نعرف $a \sim b$ إذا كان $a - b$ عددا زوجيا. سنتحقق الآن من أن هذه هي علاقة تكافؤ على S.

١ ـ بما أن العدد $a - a = 0$ هو عدد زوجي لذا فإن $a \sim a$.

٢ ـ إذا كان $a \sim b$ فإن $a - b$ عدد زوجي، وعندئذ $b - a = -(a - b)$ هو عدد زوجي أيضا ولذلك فإن $b \sim a$.

٣ ـ إذا كان $a \sim b$ و $b \sim c$ فإن كُلا من $a - b$ و $b - c$ عدد زوجي، وبالتالي فإن $a - c = (a - b) + (b - c)$ هو عدد زوجي أيضا مما يثبت أن $a \sim c$.

مثال (١ ـ ١ ـ ٣)

لنفرض أن S هي مجموعة الأعداد الصحيحة وأن $n > 1$ عدد صحيح ولنعرف لكل $a, b \in S$ العلاقة $a \sim b$ إذا كان $a - b$ مضاعف للعدد n. عندئذ تكون العلاقة $\sim$ هي علاقة تكافؤ على S وسنترك إثباتها تمرينا للقارىء.

مثال (١ ـ ١ ـ ٤)

لنفرض أن S هي مجموعة المثلثات في المستوى. عندئذ إن مثلثين في هذه المجموعة متكافئان إذا كانا متشابهين. [بمعنى أن زواياهما المتقابلة متساوية] عندئذ إن هذه العلاقة هي علاقة تكافؤ على S.

مثال (١ـ١ـ٥)

لنفرض أن S هي مجموعة النقاط في المستوى. عندئذ نُعرف تكافؤ النقطتين a,b إذا كانا على مسافة متساوية من نقطة الأصل. إنه من الواضح أن هذه هي علاقة تكافؤ على S. وكلما تقدمنا في هذا الكتاب سنواجه أمثلة كثيرة من علاقات التكافؤ.

تعريف

إذا كانت A مجموعة و ~ علاقة تكافؤ على A ، عندئذ نعرف فصل (صنف) التكافؤ (Equivalence class) للعنصر a في A بأنه المجموعة $\{x \in A / x \sim a\}$ وسنرمز له بالرمز $cl(a)$.

الآن ما هي فصول التكافؤ في الأمثلة التي ناقشناها؟

- في المثال (١ـ١ـ١) يتكون فصل التكافؤ للعنصر a من العنصر a نفسه فقط.
- في المثال (١ـ١ـ٢) يتكون فصل التكافؤ للعنصر a من جميع الأعداد الصحيحة من الصيغة $a+2m$ حيث $m=0,\pm1,\pm2,\ldots$ وفي هذا المثال يوجد فصلا تكافؤ مختلفان هما $cl(0)$ و $cl(1)$.
- في المثال (١ـ١ـ٣) يتكون فصل التكافؤ للعنصر a من جميع الأعداد الصحيحة من الصيغة $a+kn$ حيث $k=0,\pm,1,\pm2,\ldots$ ، كما أن عدد فصول التكافؤ المختلفة هو n وهي $cl(0), cl(1), \ldots cl(n-1)$.
- في المثال (١ـ١ـ٥) يتكون فصل التكافؤ للعنصر a من مجموعة النقاط في المستوى التي تقع على دائرة مركزها نقطة الأصل وتمر بالنقطة a.

على الرغم من أننا أوردنا تعاريف قليلة وكذلك بعض المفاهيم وبرهنا قضية بسيطة فإنه يمكن القول بدون مبالغة إنه حتى هذا الحد لم نبرهن أية نتيجة أساسية، ونحن الآن على وشك إثبات أول نتيجة جوهرية في هذا الكتاب. إن إثبات هذه المبرهنة ليس صعبا، بل على العكس من ذلك بسيط جدا، ولكن رغم ذلك كله فإن النتيجة التي تتضمنها، من وجهة نظرنا، سيكون لها استخدام كثير.

مبرهنة (١ - ١ - ١)

إن فصول التكافؤ المختلفة لعلاقة التكافؤ المعرّفة على المجموعة A تفرّقها إلى اتحاد مجموعات جزئية منفصلة عن بعضها البعض ومن ناحية أخرى إذا أمكن كتابة المجموعة A على هيئة اتحاد مجموعات جزئية منفصلة وغير خالية، فإنه يمكننا تعريف علاقة تكافؤ على المجموعة A بحيث تكون هذه المجموعات الجزئية هي فصول التكافؤ المختلفة.

البرهـان

لنفرض أن علاقة التكافؤ المعرفة على A هي $\sim$. نلاحظ أولا أنه لأي عنصر a في A يكـون $a\sim a$ وعليه فإن $a \in cl(a)$ وبـالتـالي فإن اتحـاد جميع فصـول التكافؤ هو A . فإذا كان لدينا فصلا تكافؤ فإننا نجزم أنهما إما متساويان أو منفصلان. ولإثبات ذلـك نفـرض أن $cl(a)$ و $cl(b)$ غير منفصلين، عنـدئـذ، يوجـد عنصر x بحيث يكـون $x\in cl(a)\cap cl(b)$. ولـما كان $x\in cl(a)$ ، فإننـا نجد أن $a\sim x$ ، وأيضا لما كان $x\in cl(b)$ فإننا نجد أيضا أن $b\sim x$. واستنادا إلى خاصة التناظر نجد أن $x\sim b$ ، وبالتالي فإن $a\sim x$ و$x\sim b$ ووفقا لخاصة التعدي نجد أن $a\sim b$.

لنفرض الآن أن $y\in cl(b)$ ، أي أن، $b\sim y$ ، ومن العلاقتين $b\sim y$ ، $a\sim b$ نستنتج أن $a\sim y$ أي أن $y\in cl(a)$ ، وبالتالي فإن كل عنصر في $cl(b)$ ينتمي إلى $cl(a)$ مما يثبت أن $cl(b)\subset cl(a)$. وبمناقشة مشابهة يتم إثبات أن $cl(a)\subset cl(b)$ ، ومن ذلك نستنتج أن $cl(a) = cl(b)$.

وبهذا نكون قد بيّنا أن فصول التكافؤ المختلفة منفصلة عن بعضها البعض وأن اتحادها هو المجموعة A . وهذا يثبت الجزء الأول من المبرهنة .

ولبرهان الاتجاه الآخر، لنفرض أن $A=\cup A_{\alpha}$ حيث المجموعات A_{α} منفصلة عن بعضها البعض وغير خالية [لاحظ أن α عنصر في مجموعة دليل ما]. إن السؤال الذي يطرح نفسه هو كيف نستخدم هذا لتعريف علاقة تكافؤ؟

إن الجواب على ذلك واضح هو أنه إذا كان a عنصرا من A فإنه ينتمي تماما إلى واحدة من المجموعات الجزئية A_{α} ، ومن أجل العنصرين b,a في A نعرف $a\sim b$ إذا كان b,a ينتميان إلى المجموعة الجزئية نفسها A_{α} . سنترك التحقق من أن هذه هي علاقة تكافؤ على A وأن فصول التكافؤ المختلفة هي المجموعات A_{α} كتمرين للقارىء .

مسائل

١ - (ا) إذا كانت A مجموعة جزئية من B وB مجموعة جزئية من C فأثبت أن A مجموعة جزئية من C .

(ب) إذا كانت $B\subset A$ فأثبت أن $A\cup B=A$ وأن العكس صحيح .

(جـ) إذا كانت $B\subset A$ فأثبت أنه لأية مجموعة C يكون $B\cap C\subset A\cap C$ وأن $B\cup C\subset A\cup C$.

٢ - (ا) أثبت أن $A\cap B=B\cap A$ وأن $B\cup A=A\cup B$.

(ب) أثبت أن $(A\cap B)\cap C = A\cap(B\cap C)$

٣ - برهن على أن $A\cup (B\cap C) = (A\cup B) \cap (A\cup C)$

٤ - إذا رمزنا لمتممة المجموعة الجزئية C من المجموعة S بالرمز C' فأثبت قانوني دي مورجان (De Morgan laws) الآتيين، وذلك للمجموعتين الجزئيتين B,A في S :

(ا) $(A\cap B)' = A'\cup B'$

(ب) $(A\cup B)' = A'\cap B'$

٥ - إذا رمزنا إلى عدد عناصر المجموعة المنتهية C بالرمز $0(C)$ وإذا فرضنا أن A و B مجموعتان منتهيتان، فعندئذ أثبت أن:

$$0(A\cup B) = 0(A) + 0(B) - 0(A\cap B)$$

٦ - أثبت أنه إذا كانت A مجموعة منتهية، عدد عناصرها n فإن عدد المجموعات الجزئية في A هو 2^n.

٧ - توضح عملية مسح أن ٦٣٪ من الأمريكيين يحبون الجبن بينما ٧٦٪ منهم يحبون التفاح. ماذا نستطيع أن نقول عن النسبة المئوية من الأمريكيين الذين يحبون الجبن والتفاح في الوقت نفسه؟ (إن الإحصائية الواردة لا تعني الإحصائية الدقيقة).

٨ - يعرف **الفرق التناظري** (Symmetric Difference) للمجموعتين A و B بأنه $(A-B)\cup(B-A)$ أثبت أن الفرق التناظري للمجموعتين A و B يساوي $(A\cup B)-(A\cap B)$.

٩ - لنفرض أن S مجموعة و S^* هي مجموعة المجموعات الجزئية المختلفة من S. ولنعرف الجمع والضرب في S^* كما يلي:

إذا كانت $A,B\in S^*$ (تذكر أن B,A مجموعتان جزئيتان في S) فإن:

$A + B = (A - B)\cup(B - A)$ ،

$A.B = A\cap B$

برهن القوانين الآتية التي تحكم هاتين العمليتين:

(ا) $(A + B) + C = A + (B + C)$

(ب) $A.(B + C) = A.B + A.C$

(جـ) $A.A = A$

(د) $A + A$ هي المجموعة المعدومة.

(هـ) إذا كان $A + B = A + C$ فإن $B = C$.

(إن النظام الموصوف بالخواص السابقة هو مثال لما يدعى بالجبر البوليني (Boolean Algebra)).

١٠ـ بيّن أيًّا من العلاقات الآتية هي علاقة تكافؤ على S

(ا) S هي مجموعة سكان العالم والعلاقة هي أن $a \sim b$ إذا كان لهما الجد الأعلى نفسه.

(ب) S هي مجموعة سكان العالم والعلاقة هي أن $a \sim b$ إذا كان a يسكن على بعد ١٠٠ ميل من b .

(جـ) S هي مجموعة سكان العالم والعلاقة هي أن $a \sim b$ إذا كان لهما الأب نفسه.

(د) S هي مجموعة الأعداد الحقيقية والعلاقة هي أن $a \sim b$ إذا كان $a = \pm b$.

(هـ) S هي مجموعة الأعداد الصحيحة والعلاقة هي أن $a \sim b$ إذا تحققت كل من العلاقتين $a > b$ و $b > a$

(و) S هي مجموعة الخطوط المستقيمة في المستوى والعلاقة هي أن $a \sim b$ إذا كان a يوازي b .

١١ـ (ا) تنص الخاصتان الثانية والثالثة من خواص علاقة التكافؤ على أنه إذا كان $a \sim b$ فإن $b \sim a$ وإذا كان $a \sim b$ و $b \sim c$ فإن $a \sim c$. الآن ما هو الخطأ في البرهان الآتي لإثبات أن الخاصتين الثانية والثالثة تؤديان إلى الخاصة الأولى؟ لنفرض أن $a \sim b$ ، عندئذ $b \sim a$ واستنادًا إلى الخاصة الثالثة (مفترضين أن $a = c$) نجد أن $a \sim a$.

(ب) هل يمكنك اقتراح بديل للخاصة الأولى والذي سيضمن لنا أن الخاصتين الثانية والثالثة تقتضيان فعلًا الخاصة الأولى؟

١٢- في المثال (١-١-٣) من أمثلة علاقات التكافؤ أثبت أن تلك العلاقة هي علاقة تكافؤ، كما أن عدد فصول التكافؤ المختلفة هو n وهي cl(0), cl(1),...., cl(n-1)

١٣- أكمل برهان الجزء الثاني من مبرهنة (١-١-١).

(١ - ٢) التطبيقـات

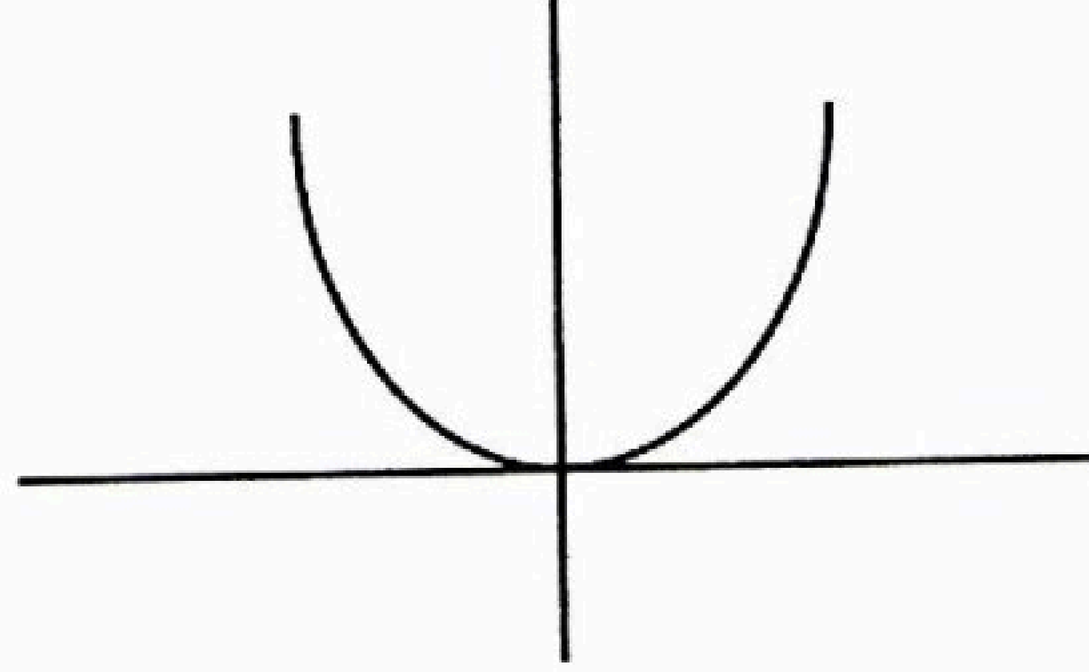
نحن الآن على وشـك إدخـال مفهوم التطبيق من مجموعة إلى أخرى ويمكن القول، بدون أية مبالغة، إن هذا المفهوم هو من أهم المفاهيم المستخدمة في جميع فروع الرياضيات، وأنه ليس جديدا علينا، حيث كنا ندرس التطبيقات منذ بداية تَعَلُّمِنا للرياضيات. فعندما كان يطلب منا رسم العلاقة $y=x^2$، كان ببساطة يطلب أن ندرس التطبيق الذي ينقل كل عدد حقيقي إلى مربعه.

بتعبير غير دقيق، يمكننا القول بأن التطبيق من مجموعة S إلى مجموعة أخرى T هو قاعدة - مهما كان يعني ذلك - تربط كل عنصر s من S بعنصر وحيد t من T .

سنعـرف التـطبيق بطريقة أكثر دقة ومنهجية والغرض من ذلك هو السماح لنا بالتفكير والحديث على ضوء الشروط السابقة. إنه يمكن اعتبار التطبيق على أنه قاعدة أو طريقة أو آلة تنقلنا من مجموعة إلى أخرى.

دعنـا نمهد قليلاً للتعريف الذي سنورده. إن وجهة النظر التي سنتبناها هي اعتبار التطبيق معرف «برسمه». وسنوضح هذا المثال المألوف ($y=x^2$) معرفا على مجموعة الأعداد الحقيقية والذي يأخذ قيمه في S . ومن أجل S تكون S×S هي مجموعة جميع النقاط (a,b) التي يمكن أن نعتبرها على أنها المستوى، حيث يقابل الزوج (a,b) النقطة التي إحداثياتها b,a على الترتيب. في هذا المستوى سنختار جميع النقاط التي إحداثياتها من الشكل (x,x^2) وسنطلق على هذه المجموعة رسم العلاقة $y=x^2$.

ويمكن تمثيل هذه المجموعة بالرسم كما يلي:



ولكي نحدد قيمة التطبيق أو الدالة عند النقطة $x = a$ ننظر في الرسم إلى النقطة التي إحداثيها الأول هو a ، ونقرأ الإحداثي الثاني على أنه قيمة الدالة عند النقطة $x=a$.

إن هذا هو المنـطلق الـذي سنستخدمه في الحالة العامة لتعريف التطبيق من مجموعة إلى أخرى.

تعريـف:

*إذا كانت T,S مجموعتين غير خاليتين، فإن **التطبيق** (mapping) من S إلى T عبارة عن مجمـوعة جزئية M من $S\times T$ ، بحيث يقابل كل عنصر $s\in S$ عنصرا وحيدا t في T ، بحيث ينتمي الزوج المرتب (s,t) إلى M .*

إن هذا التعريف يجعل مفهوم التطبيق أكثر دقة بالنسبة لنا. ورغم ذلك فإننا لن نستخدمه في صيغته هذه. وعوضا عن ذلك، نفضل اعتبار التطبيق كقاعدة تربط أي عنصر s في S بعنصر ما t في T ، هذه القـاعـدة تربط ـ أو تقـرن ـ العنصر s في S بالعنصر t في T (إذا وفقط) إذا كان (s,t) عنصرا في M . وعندها نقول إن t هو صورة العنصر s تحت تأثير هذا التطبيق.

الآن نعبِّر عما سبق باستخدام الرموز. ليكن σ هو التطبيق من S إلى T ؛ ومن وقت لآخر سنكتب ذلك بالشكل $\sigma:S\rightarrow T$ أو $S\xrightarrow{\sigma}T$. وإذا كانت t هي صورة s تحت

تأثير σ فإننا سنكتب ذلك أحيانا على الشكل $\sigma:s\rightarrow t$ وفي أغلب الأحيان سنكتبه على الصيغة $t=s\sigma$. **لاحظ هنا أننا كتبنا التطبيق σ على اليمين، ولكنه لا يوجد اتفاق عام** على كتابة التطبيق فكثير من المؤلفين يكتبه على الشكل $t=\sigma(s)$ ، وغالبا ما يكتب الجبريون التطبيق على اليمين بينما يكتبه كثير من الرياضيين الآخرين على اليسار. وفي الواقع، سوف لا نُلْزِمْ أنفسنا بذلك مطلقا، ولكن عندما نريد التأكيد على الطبيعة الدالية للتطبيق σ فإننا سنكتبه على الشكل $t=\sigma(s)$.

أمثلة على التطبيقات

سنفترض في جميع الأمثلة الآتية أن المجموعات غير خالية.

مثال (١-٢-١)

لنفرض أن S أي مجموعة ولنعرف $\iota:S\rightarrow S$ بالقاعدة $s=s\iota$ لأي عنصر s في S . يطلق على هذا التطبيق ι **بالتطبيق المحايد** (Identity mapping) على S .

مثال (١-٢-٢)

إذا كانت T,S أي مجموعتين وكان $t_0 \in T$. ولنعرف $\tau:S\rightarrow T$ بالقاعدة $\tau:s\rightarrow t_0$ لكل s في S .

مثال (١-٢-٣)

لنفرض أن S هي مجموعة الأعداد النسبية، وأن $T=Z\times Z$ حيث Z هي مجموعة الأعداد الصحيحة. عندئذ إذا كان s هو أي عدد نسبي فإن بإمكاننا كتابته على الصيغة $s=\frac{m}{n}$ حيث لا يوجد عامل مشترك بين العددين m و n . لنعرف $\tau:S\rightarrow T$ كما يلي: $s\tau=(m,n)$.

مثال (١-٢-٤)

لنفرض أن Z هي مجموعة الأعداد الصحيحة وأن:

$$S=\{(m,n)\in Z\times Z \mid n\neq 0\}$$

ولنفـرض أن T هي مجمـوعـة الأعـداد النسبية ولنعـرف $\tau:S\to T$ بالقـاعـدة $(m,n)\tau=\frac{m}{n}$ ، لكل $(m,n)\in S$.

مثال (١-٢-٥)

لنفـرض أن Z هي مجموعة الأعداد الصحيحة وأن $S = Z\times Z$ ولنعرف $\tau:S\to Z$ بالقاعدة $(m,n)\tau = m+n$.

لاحظ أنـه في المثـال (١-٢-٥) يمكن اعتبـار الجمع في Z على أنه تطبيق من Z×Z إلى Z . إذا كانت S مجمـوعـة ما فإننـا نسمي التطبيق من S×S إلى S **عملية ثنائية** (Binary operation) على S . فإذا كان لدينا مثل هذا التطبيق $\tau:S\times S\to S$ ، فإن باستـطاعتنـا استخـدامـه لتعـريف «الضرب» * على S وذلك بكتابة $a*b=c$ إذا كان $(a,b)\tau = c$.

مثال (١-٢-٦)

لنفـرض أن T,S أي مجموعتين ولنعرف $\tau:S\times T\to S$ بالقاعدة $(a,b)\tau = a$ لأي عنصر $(a,b)\in S\times T$. إن هذا التـطبيق يدعى **بإسقـاط** (Projection) S×T على S . وبطريقة مماثلة يمكن تعريف إسقاط S×T على T .

مثال (١-٢-٧)

لنفـرض أن S هي المجموعة التي عناصرها x_1,x_2,x_3 ولنعرف $\tau:S\to S$ كما يلي : $x_1\tau=x_2$ ، $x_2\tau=x_3$ ، $x_3\tau=x_1$.

مثال (١-٢-٨)

لنفرض أن S هي مجموعة الأعداد الصحيحة وT هي المجموعة التي عناصرها E و O . ولـنـعــرف $\tau:S\to T$ بالـقــاعــدة $n\tau=E$ إذا كان n زوجيا و $n\tau=O$ إذا كان n فرديا(*) .

(*) لاحظ أن اختيار الحرفين O,E يعود إلى أنهما أول حرفين في الكلمتين Even و Odd اللتين تعنيان زوجيا وفرديا على التوالي . (ملاحظة المترجمين) .

الآن لنفرض أن S هي أية مجموعة، وأن $\{x_1,...,x_n\}$ مجموعة جزئية من S عناصرها هي $x_1,x_2,...,x_n$. وبصورة خاصة $\{x\}$ هي المجموعة الجزئية من S التي تتكون من عنصر واحد هو x . عندئذ يمكننا استخدام المجموعة S لبناء مجموعة جديدة S^* عناصرها مجموعات S الجزئية. يطلق على S^* **مجموعة المجموعات الجزئية في S** . فعلى سبيل المثال إذا كانت $S=\{x_1, x_2\}$ فإن S^* تحتوي على أربعة عناصر هي المجموعة الخالية ϕ ولنرمز لها بالرمز a_1 والمجموعة a_2 التي هي S و$a_3=\{x_1\}$ و $a_4=\{x_2\}$
إن علاقة S بالمجموعة S^* مهمة بصورة عامة وسنوضح بعض خواصها في المسائل.

مثال (١-٢-٩)

لنفرض أن S أية مجموعة وأن $T=S^*$ ، ولنعرف $\tau:S\to T$ بأنه ينقل العنصر s إلى متممة $\{s\}$ والتي تساوي $S-\{s\}$.

مثال (١-٢-١٠)

لنفرض أن S مجموعة معرف عليها علاقة تكافؤ وأن T هي مجموعة فصول التكافؤ في S (لاحظ أن T مجموعة جزئية في S^*) ولنعرف $\tau:S\to T$ بالقاعدة $s\tau=cl(s)$.

نعود الآن إلى مناقشة الموضوع ولنفرض أن $\tau:S\to T$ تطبيق ولنعرف **الصورة العكسية** (Inverse image) للعنصر $t\in T$ بأنها المجموعة $\{s\in S|t=s\tau\}$. إن الصورة العكسية للعنصر E في المثال (١-٢-٨) هي المجموعة الجزئية من S التي تتكون من الأعداد الزوجية. قد يحدث أن تكون الصورة العكسية لعنصر $t\in T$ تحت تأثير τ هي المجموعة الخالية. بمعنى أن t ليس صورة لأي عنصر من S تحت تأثير τ . ففي المثال (١-٢-٣) نجد أن العنصر (4,2) ليس صورة لأي عنصر من S تحت تأثير τ كما أن العنصر S في المثال (١-٢-٩) باعتباره عنصرا من S^* ليس صورة لأي عنصر من S تحت تأثير τ .

تعريف

يقال عن التطبيق τ من المجموعة S إلى المجموعة T إنه ***تطبيق غامر (على) (onto)*** *إذا كان يوجد لكل $t\in T$ عنصر $s\in S$ بحيث يكون $s\tau=t$.*

ويمكن التعبير عن ذلك بقولنا إن التطبيق $\tau:S\to T$ هو تطبيق غامر إذا كانت المجموعة $S\tau=\{x\in T|x=s\tau;s\in S\}$ ، والتي يطلق عليها صورة S تحت تأثير τ هي كل T

لاحظ أن التطبيقات في الأمثلة (١-٢-١)، (١-٢-٤)، (١-٢-٥)، (١-٢-١٠) كلها تطبيقات غامرة.

وفيما يلي، نُعَرِّف نوعا خاصا ومهما من التطبيقات التي كثيرا ما تقابلنا، ذلك هو ما يطلق عليه **التطبيق الأحادي**.

تعريف

يقال عن التطبيق τ من المجموعة S إلى المجموعة T إنه ***تطبيق أحادي*** *(one-to-one) عندما يكون $s_1 \neq s_2$ يقتضي أن $s_1\tau\neq s_2\tau$.*

ويمكن القـول بأن التـطبيق τ هو تطبيق أحادي إذا كانت الصورة العكسية لعنصر t في T هي المجموعة الخالية أو المجموعة التي تتكون من عنصر واحد.

إن التطبيقات الواردة في الأمثلة (١-٢-١) ، (١-٢-٣)، (١-٢-٧)، (١-٢-٩) جميعها تطبيقات أحادية.

الآن متى نستطيع أن نقول إن التطبيقين من S إلى T متساويان؟
إن الجواب على ذلك هو أنه يجب أن يكون لهما التأثير نفسه على كل عنصر من S بمعنى أن صورة أي عنصر من S تحت تأثير أيٍّ من التطبيقين هي نفسها.

والآن نعرف تساوي تطبيقين بدقة أكثر.

تعريف

يقال إن التطبيقين τ و σ من S إلى T ***متساويان*** *إذا كان $s\sigma = s\tau$ لكل s في S.*

لنعتبر الآن الوضع التالي، إذا كان σ تطبيقا من S إلى T ، و τ تطبيقا من T إلى U فهل نستطيع تركيب هذين التطبيقين والحصول على تطبيق من S إلى U ؟ إن الطريقة الطبيعية والواضحة هي نقل عنصر $s\in S$ إلى U وفق خطوتين أولاهما تطبيق σ على s ثم تطبيق τ على العنصر الناتج $s\sigma$ في T . إن ما سبق يمكن اعتباره أساسا للتعريف التالي.

تعريف

*إذا كان $\sigma:S\to T$ و $\tau:T\to U$ ، **فإن تركيب** (Composition) σ مع τ (ويدعى أيضا حاصل ضربهما) هو التطبيق $\sigma\circ\tau:S\to U$ المعروف بالقاعدة $s(\sigma\circ\tau) = (s\sigma)\tau$ وذلك لكل $s\in S$.*

نلاحظ من هذا التعريف أن تركيب التطبيقين يقرأ من اليسار إلى اليمين أي $\sigma\circ\tau$ ، أي أننا نبدأ بالتطبيق σ ثم نتبعه بالتطبيق τ . هنا نجد أن قضية اليمين واليسار ليست ثابتة.

إن الرياضيين الذين يكتبون التطبيقات على اليسار سيقرؤون التركيب $\sigma\circ\tau$ على أنه يعني التطبيق τ أولا ثم يتبعونه بالتطبيق σ . ووفقا لذلك، يجب على أي فرد أن ينتبه عند قراءة كتاب في الرياضيات، إلى الطريقة المتبعة في كتابة تركيب تطبيقين. وبالنسبة لنا فإننا نكرر القول «بأن $\sigma\circ\tau$ يعني دائما بالنسبة لنا تطبيق σ أولا ثم τ ».

نوضح الآن تركيب التطبيقين ببعض الأمثلة.

مثال (١-٢-١١)

لنفرض أن $S=\{x_1, x_2, x_3\}$ و أن $T=S$ وأن $\sigma:S\to S$ معرف وفق القاعدة:

$$x_1\sigma=x_2,\ x_2\sigma=x_3,\ x_3\sigma=x_1$$

وأن τ معرف بالقاعدة:

$$x_1\tau=x_1,\ x_2\tau=x_3,\ x_3\tau=x_2$$

عنـدئـذ:

$$x_1(\sigma\circ\tau)=(x_1\sigma)\,\tau= x_2\tau=x_3$$
$$x_2(\sigma\circ\tau)=(x_2\sigma)\,\tau= x_3\tau=x_2$$
$$x_3(\sigma\circ\tau)=(x_3\sigma)\,\tau= x_1\tau=x_1$$

كما نستطيع حساب $\tau\circ\sigma$ كما يلي:

$$x_1(\tau\circ\sigma)=(x_1\tau)\,\sigma= x_1\sigma=x_2,$$
$$x_2(\tau\circ\sigma)=(x_2\tau)\,\sigma= x_3\sigma=x_1,$$
$$x_3(\tau\circ\sigma)=(x_3\tau)\,\sigma= x_2\sigma=x_3$$

لاحظ هنا أن $x_1(\tau\circ\sigma) = x_2$ بينما $x_3=x_1(\sigma\circ\tau)$ وبالتالي فإن $\sigma\circ\tau \neq \tau\circ\sigma$

مثال (١-٢-١٢)

لنفرض أن S هي مجموعة الأعداد الصحيحة وأن $T=S\times S$ وأن $\sigma:S\to T$ معرف وفق القـاعـدة $m\sigma=(m-1,1)$. لنفرض أيضا أن $U=S$ ، وأن $\tau:T\to U(=S)$ معرف بالقاعدة $(m,n)\tau=m+n$.

عندئذ $\sigma\circ\tau: S\to S$ ، بينما $\tau\circ\sigma:T\to T$.

إن الحـديث عن تسـاوي $\sigma\circ\tau$ و $\tau\circ\sigma$ غير وارد في هذه الحـالـة، ذلـك لأنهما لا يؤثـران على المجمـوعة نفسها. والآن نحسب $\sigma\circ\tau$ كتطبيـق مـن S إلى نفسها ثم $\tau\circ\sigma$ كتطبيق من T إلى نفسها.

لنفرض أن $m\in S$ عندئذ $m\sigma = (m-1,1)$ وبالتالي: فإن:

$$m\,(\sigma\circ\tau) = (m\sigma)\,\tau = (m-1,1)\,\tau = (m-1) + 1 = m$$

أي أن $\sigma\circ\tau$ هو التـطبيق المحـايد من S إلى نفسهـا. والآن ماذا يمكن أن نقـول عن $\tau\circ\tau$ ؟

لنفرض أن $(m,n)\in T$ ، عندئذ $(m,n)\tau=m+n$ بينما

$$(m,n)\,(\tau\circ\sigma) = \big((m,n)\tau\big)\,\sigma = (m+n)\,\sigma = (m+n-1,1)$$

لاحظ أن $\sigma\circ\tau$ ليس تطبيقا محايدا من T إلى نفسها، وفضلا عن ذلك، فإنه ليس تطبيقا غامرا من T إلى نفسها.

مثال (١-٢-١٣)

لنفرض أن S هي مجموعة الأعداد الحقيقية، وأن T هي مجموعة الأعداد الصحيحة وأن $U=\{E,O\}$. ولنعرف $\sigma:S\to T$ بالقاعدة وهي أن $s\sigma$ هي أكبر عدد صحيح يقل عن s أو يساويه، وأن $\tau:T\to U$ معرف بالقاعدة.

$$n\tau = \begin{cases} E & \text{إذا كان } n \text{ زوجيا} \\ O & \text{إذا كان } n \text{ فرديا} \end{cases}$$

لاحظ هنا أن $\tau\circ\sigma$ غير معرف. نحسب صورة العددين الحقيقيين $s=\pi$ ، $s=8/3$ وذلك تحت تأثير $\sigma\circ\tau$. لما كان، $s=8/3=2+2/3$ لذلك فإن $(8/3)\sigma=2$ ، بينما $(8/3)(\sigma\circ\tau)=(8/3\sigma)\tau=2\tau=E$ كذلك فإن $(\pi)\sigma=3$ ،

بينما $\pi(\sigma\circ\tau)=(\pi\sigma)\tau=(3)\tau=0$

إن التطبيقات بصورة عامة تحقق قانون التجميع بشرط أن يكون لتركيب التطبيقات معنى. وهذا ما تنص عليه التمهيدية الآتية.

تمهيدية (١-٢-١) (قانون التجميع)

إذا كان $\sigma:S\to T$ ، $\tau:T\to U$ و $\mu:U\to V$ فإن

$$(\sigma\circ\tau)\circ\mu=\sigma\circ(\tau\circ\mu)$$

البرهان

لاحظ أولا أن للتطبيق $\sigma\circ\tau$ معنى كما أنه يصوِّر S إلى U ، ومن ثم فإن للتطبيق $(\sigma\circ\tau)\circ\mu$ معنى أيضا حيث يصوِّر S إلى V . وبالمثل فإن للتطبيق $\sigma\circ(\tau\circ\mu)$ معنى حيث يصوِّر S إلى V . وعليه نستطيع التحدث عن تساوي التطبيقين $(\sigma\circ\tau)\circ\mu$ ، $\sigma\circ(\tau\circ\mu)$ أو عدم تساويهما.

لكي نثبت المساواة المطلوبة، علينا أن نثبت أنه لأي s في S يكون

$$s((\sigma\circ\tau)\circ\mu) = s(\sigma\circ(\tau\circ\mu))$$

فباستخدام تعريف تركيب التطبيقات يكون لدينا

$$s((\sigma\circ\tau)\circ\mu) = (s(\sigma\circ\tau)\mu = ((s\sigma)\tau)\mu$$

بينما

$$s(\sigma o(\tau\circ\mu)) = (s\sigma)(\tau\circ\mu) = ((s\sigma)\tau)\mu$$

وبالتالي فإن العنصرين $s((\sigma\circ\tau)\circ\mu)$ ، $S(\sigma o(\tau\circ\mu))$ متساويان بالفعل، وهذا ما يثبت المطلوب.

نود الآن إثبات أنه إذا كان لدينا تطبيقان يحققان شروطا معيّنة فإن تركيبهما يحقق الشروط نفسها.

تمهيدية (١-٢-٢)

إذا كان $\sigma:S\to T$ و $\tau:T\to U$ فإن:

(١) *$\sigma\circ\tau$ غامر إذا كان كل من σ و τ غامرا.*

(٢) *$\sigma\circ\tau$ أحادي إذا كان كل من σ ، τ أحاديا.*

البرهان

سنثبت القسم الثاني تاركين برهان القسم الأول كتمرين للقارىء. لنفرض أن $s_1, s_2 \in S$ وأن $s_1 \neq s_2$ عندئذ $s_1\sigma \neq s_2\sigma$ لأن σ أحادي. كذلك، لما كان $s_1\sigma \neq s_2\sigma$ ، وأيضا لما كان τ أحاديا لذلك فإن $(s_1\sigma)\tau \neq (s_2\sigma)\tau$ ، وبالتالي فإن

$$s_1(\sigma\circ\tau) = (s_1\sigma)\tau \neq (s_2\sigma)\tau = s_2(\sigma\circ\tau)$$

مما يثبت أن $\sigma\circ\tau$ أحادي، وبهذا يتم المطلوب.

لنفرض الآن أن σ تطبيق أحادي من S على T ، عندئذ يطلق على σ أنه تقابل بين T,S . لنفرض الآن أن $t \in T$. ولما كان σ غامرا، لذا فإنه يوجد عنصر $s \in S$ بحيث يكون $t=s\sigma$ ، وأيضا لما كان σ أحاديا لذا فإن العنصر s وحيد.

الآن نعرف التطبيق $\sigma^{-1}:T\rightarrow S$ بالقاعدة $s=t\sigma^{-1}$ إذا وفقط إذا كان $t=s\sigma$. يطلق على التطبيق σ^{-1} معكوس σ ؛ الآن نحسب $\sigma\circ\sigma^{-1}$ الذي ينقل S إلى نفسها. لنفرض أن $s\in S$ وأن $t=s\sigma$ ، عندئذ من التعريف $s=t\sigma^{-1}$ يكون:

$$s(\sigma\circ\sigma^{-1}) = (s\sigma)\sigma^{-1}= t\sigma^{-1}=s$$

أي أن التطبيق $\sigma\circ\sigma^{-1}$ هو التطبيق المحايد من S على نفسها. وبطريقة مماثلة يتضح لنا أن $\sigma^{-1}\circ\sigma$ هو التطبيق المحايد من T على نفسها.

ومن ناحية أخرى، إذا كان $\mu:T\rightarrow S, \sigma:S\rightarrow T$ تطبيقا بحيث يكون كل من $\sigma\circ\mu$ و $\mu\circ\sigma$ التطبيق المحايد على كل من T,S على الترتيب، فإننا ندعي أن σ تقابل بين T,S . لإثبات ذلك نلاحظ أولا أن σ غامر، لأنه إذا كان $t\in T$ فإن $t=t(\mu\circ\sigma)=(t\mu)\sigma$ لأن $\mu\circ\sigma$ هو التطبيق المحايد على T وبالتالي t هو صورة العنصر $t\mu\in S$ تحت تأثير σ . كذلك لاحظ أن σ أحادي لأنه إذا كان $s_1\sigma=s_2\sigma$ ، وبما أن $\sigma\circ\mu$ هو التطبيق المحايد على S ، لذلك نجد أن

$$s_1 = s_1(\sigma\circ\mu) = (s_1\sigma)\,\mu = (s_2\sigma)\,\mu = s_2\,(\sigma\circ\mu) = s_2$$

بهذا نكون قد أثبتنا التمهيدية الآتية.

تمهيدية (١-٢-٣)

يكون التطبيق $\sigma:S\rightarrow T$ تقابلا بين T,S إذا وفقط إذا كان يوجد تطبيق $\mu:T\rightarrow S$ بحيث يكون $\sigma\circ\mu$ و $\mu\circ\sigma$ هما التطبيقان المحايدان على كل من T,S على الترتيب.

تعريف

إذا كانت S مجموعة غير خالية فإن $A(S)$ هي مجموعة كل التقابلات من S على نفسها.

إنه علاوة على أهمية $A(S)$ الجوهرية، فإنها تلعب دورا بارزا في البناء الرياضي المعروف بالزمرة، كما سنرى ذلك في الفصل الثاني. ولهذا نذكر نص المبرهنة الآتية التي توضح طبيعة $A(S)$ بدون برهان حيث برهنا جميع فقراتها في التمهيديات السابقة.

مبرهنة (١-٢-١)

إذا كان $\sigma,\tau,\mu\in A(S)$

فإن:

(١) $\sigma\circ\tau\in A(S)$

(٢) $\sigma\circ(\tau\circ\mu)=(\sigma\circ\tau)\circ\mu$

(٣) يوجد عنصر ι في (التطبيق المحايد على S) في $A(S)$ بحيث يكون $\sigma\circ\iota=\iota\circ\sigma=\sigma$

(٤) يوجد عنصر σ^{-1} في $A(S)$ بحيث يكون $\sigma^{-1}\circ\sigma=\sigma\circ\sigma^{-1}=\iota$.

ونختتم هذا البند بملاحظة حول $A(S)$. لنفرض أن S تحتوي على أكثر من عنصرين وأن x_3, x_2, x_1 ثلاثة عناصر مختلفة من S، ولنعرف التطبيق $\sigma:S\to S$ كما يلي $x_1\sigma=x_2, x_2\sigma=x_3, x_3\sigma=x_1$ و $s\sigma=s$ لكل عنصر s في S مختلف عن x_1 ، x_2 و x_3.

كذلك لنعرف التطبيق $\tau:S\to S$ كما يلي $x_2\tau=x_3$ و $x_3\tau=x_2$ و $s\tau=s$ لأي عنصر s في S مختلف عن x_2 و x_3 . إن من الواضح أن σ و τ عنصران من $A(S)$ ، كذلك فإن حسابا بسيطا يثبت أن $x_1(\sigma\circ\tau)=x_3$ ولكن $x_1(\tau\circ\sigma)=x_2\neq x_3$ مما يثبت أن $\sigma\circ\tau\neq\tau\circ\sigma$.
وهذا بدوره يقودنا إلى التمهيدية التالية:

تمهيدية (١-٢-٤)

إذا كانت المجموعة S تحتوي على أكثر من عنصرين فإن باستطاعتنا إيجاد عنصرين σ و τ في $A(S)$ بحيث يكون $\sigma \circ \tau \neq \tau \circ \sigma$.

مسائل

١ - عيّن فيما إذا كان $\sigma : S \to T$ تطبيقا غامرا أو أحاديا أو غامرا وأحاديا معا ثم عيّن الصورة العكسية لأي عنصر t في T تحت تأثير τ وذلك في الحالات الآتية:

(ا) S = مجموعة الأعداد الحقيقية و T = مجموعة الأعداد الحقيقية غير السالبة و $s\sigma = s^2$.

(ب) $T=S$ = مجموعة الأعداد الحقيقية غير السالبة و $s\sigma = s^2$.

(جـ) $T=S$ = مجموعة الأعداد الصحيحة و $s\sigma = s^2$.

(د) $T=S$ = مجموعة الأعداد الصحيحة و $s\sigma = 2s$.

٢ - إذا كانت T,S مجموعتين غير خاليتين، فبرهن على وجود تقابل بين $S \times T$ و $T \times S$.

٣ - إذا كانت U, T, S ثلاث مجموعات غير خالية فبرهن على وجود تقابل بين:

(ا) $(S \times T) \times U$ و $S \times (T \times U)$

(ب) أي من المجموعتين في (ا) ومجموعة الثلاثي المرتب (s,t,u) حيث $s \in S$ و $t \in T$ و $u \in U$.

٤ - (ا) إذا كان يوجد تقابل بين T,S فأثبت وجود تقابل بين S,T .

(ب) إذا كان يوجد تقابل بين T,S وبين U,T فأثبت وجود تقابل بين U,S .

٥ - إذا كان i هو التطبيق المحايد على S فأثبت أنه لأي σ في $A(S)$ يكون $\sigma \circ i = i \circ \sigma = \sigma$

٦ - إذا كانت S أية مجموعة فأثبت أن من المستحيل إيجاد تطبيق غامر من S إلى S^* .

٧ - إذا كانت S تحتوي على عناصر عددها n فأثبت أن $A(S)$ تحتوي على عناصر عددها $n!$.

٨ - إذا كانت S تحتوي على عدد منته من العناصر فأثبت مايلي:

(ا) إذا كان $\sigma : S \to S$ غامرا فإنه أحادي .

(ب) إذا كان σ أحاديا من S إلى نفسها فإنه غامر.

(جـ) أورد مثالا تثبت فيه أن كلا من الجزئين السابقين غير صحيحين، وذلك عندما تحتوي S على عدد غير منتهٍ من العناصر.

٩ ـ أثبت أن معكوس كل من جزئي التمهيدية (١-٢-٢) غير صحيح، أي:

(ا) إذا كان $\sigma\circ\tau$ غامرا فليس من الضروري أن يكون كل من σ,τ غامرا.

(ب) إذا كان $\sigma\circ\tau$ أحاديا فليس من الضروري أن يكون كل من σ,τ أحاديا.

١٠ـ برهن على وجود تقابل بين مجموعة الأعداد الصحيحة ومجموعة الأعداد النسبية (القياسية).

١١ـ إذا كان $\sigma:S\to T$ تطبيقا من S إلى T وكانت $A\subset S$ وكان σ_A هو **اقتصار** σ (restriction) على A معرف بالقاعدة $a\sigma_A = a\sigma$ لأي a في A فأثبت مايلي:

(ا) σ_A يعرف تطبيقا من A إلى T .

(ب) إذا كان σ أحاديا فإن σ_A كذلك.

(جـ) يمكن أن يكون σ_A أحاديا حتى ولو لم يكن σ أحاديا.

١٢ـ إذا كان $\sigma:S\to S$ و $A\subset S$ بحيث يكون $A\sigma\subset A$ فأثبت أن $(\sigma\circ\sigma)_A = \sigma_A\circ\sigma_A$.

١٣ـ يقال إن المجموعة S **غير منتهية** (infinite) إذا كان يوجد تقابل بينها وبين مجموعة جزئية فعلية منها. أثبت أن:

(ا) مجموعة الأعداد الصحيحة غير منتهية.

(ب) مجموعة الأعداد الحقيقية غير منتهية.

(جـ) إذا كانت S مجموعة تحتوي على مجموعة جزئية غير منتهية فإن S يجب أن تكون غير منتهية. (**ملاحظة**: وفقا لنتيجة المسألة ٨ فإن المجموعة المنتهية بالمعنى الشائع ليست غير منتهية).

١٤* ـ إذا كانت S مجموعة غير منتهية وكان بالإمكان إيجاد تقابل بينها وبين مجموعة الأعداد الصحيحة فأثبت وجود تقابل بين S و$S\times S$.

١٥* ـ إذا كانت T,S مجموعتين فإننا نقول إن $S<T$ (S أصغر من T) إذا وُجِدَ تطبيق غامر من T إلى S ولا يوجد تطبيق غامر من S إلى T. أثبت أنه إذا كانت $S<T$ و $T<U$ فإن $S<U$.

١٦- إذا كانت T,S مجموعتين منتهيتين وكان عدد عناصرهما هو n,m على الترتيب فأثبت أنه إذا كان $m<n$ فإن $S<T$.

(١-٣) الأعداد الصحيحة

نختتم هذا الفصل بمناقشة موجزة لمجموعة الأعداد الصحيحة التي لن نحاول بناءها بطريقة المسلمات، لكننا سنفترض بدلا من ذلك أن لدينا هذه المجموعة وأننا نعلم بعض خواصهـا الأولية. سنُضَمِّنَ هذا البند مبدأ الاستقراء الرياضي (والذي سيستخدم خلال هذا الكتاب) كما سنُضَمِّنه الحقيقة التي تنص على أن مجموعة الأعداد الصحيحة الموجبة تحوى عنصرا أصغر. أما فيما يختص بالرموز، فإن الرموز المألوفة مثل $a>b$ و $a\leq b$ و $|a|$ . . . الخ. ستبقى بنفس المعنى. و لكي نتحاشى تكرار كون عدد ما صحيحـا فإننا سنفترض أن **جميع الرموز الواردة في هذا البند والمكتوبة بحروف لاتينية صغيرة تعني الأعداد الصحيحة**.

إذا كان لدينا العددان b,a وكان $b\neq 0$ ، فإن بإمكاننا أن نقسم a بواسطة b لكي نحصل على باقي r الذي هو أصغر من b ، وبعبارة أخرى، نستطيع إيجاد r,m بحيث يكون $a=mb+r$ ، حيث $0\leq r<|b|$. إن هذه هي الحقيقة المعروفة **بالخوارزم الإقليدي** (Euclidean algorithm) التي سنفترض سلفا أنها مألوفة لدينا.

كذلك، نقول إن b حيث $b\neq 0$ يقسم a إذا كان $a=mb$ ، m عددا صحيحا، وسنرمز لكون b يقسم a بالرمز $b|a$. وسنرمز لخلاف ذلك بالرمز $b\nmid a$. نلاحظ أيضا أنه إذا كان $a|1$ فإن $a=\pm 1$ ، وأيضا إذا كان $b|a$ و $a|b$ فإن $a=\pm b$ ، ونلاحظ أيضا أن أي عدد b هو قاسم للصفر. إذا كان $b|a$ فإننا نسمي b **قاسما** (divisor) للعدد a . بالإضافة إلى ذلك، نلاحظ أنه إذا كان b قاسما للعددين h,g ، فإنه قاسم كذلك للعدد $mg+nh$ حيث n,m عددان صحيحان. وسنترك برهان كل هذه الملاحظات كتمرين للقارىء.

تعريف

يقال إن العدد الصحيح الموجب c **قاسم مشترك أعظم** *(Greatest common divisor) للعددين b,a إذا كان*

(١) c قاسم لكل من b,a .

(٢) أي قاسم للعددين b,a هو قاسم للعدد c .

سنرمز للقاسم المشترك الأعظم للعددين b,a بالرمز (a,b) . وحيث إن القاسم المشترك الأعظم يجب أن يكون عددا موجبا، لذا فإننا نجد

$$(a,b) = (a,-b) = (-a,b) = (-a,-b)$$

فمثلا

$$(60,24) = (60,-24) = 12$$

ملاحظة أخرى، هي أننا عرفنا القاسم المشترك الأعظم، إلا أن هذا لا يعني أنه موجود. وإنما يجب برهان هذه الحقيقة، ومع ذلك فيمكن القول إنه إذا كان موجودا فإنه وحيد، لأنه إذا كان لدينا العددان c_2, c_1 اللذان يحققان كلا من شرطي التعريف السابق فإن $c_1|c_2$ و $c_2|c_1$ وبالتالي فإن $c_1=\pm c_2$. وحيث إن القاسم المشترك الأعظم يجب أن يكون عددا موجبا، لذلك نجد أن $c_1=c_2$. وبهذا نكون قد برهنا على وحدانية القاسم المشترك الأعظم. والآن، علينا أن نثبت وجود (a,b) . في التمهيدية التالية سنثبت أكثر من ذلك وهو أن (a,b) يجب أن يأخذ صيغة معيّنة.

تمهيدية (١-٣-١)

إذا كان b,a عددين صحيحين لا يساويان الصفر فإنه يوجد لهما قاسم مشترك أعظم (a,b) . وفضلا عن ذلك فإنه يوجد عددان صحيحان n_0, m_0 بحيث يكون

$$(a,b) = m_0a + n_0b$$

البرهان

لنفرض أن M هي مجموعة كل الأعداد الصحيحة من الصيغة ma+nb ، حيث إن n,m عددان صحيحان. وحيث إن أحد العددين b,a لا يساوي صفرا، لذلك فإن

أعدادا صحيحة غير صفرية توجد في M . ولما كان $x=ma+nb\in M$ ، لذا فإن $-x=(-m)a+(-n)b\in M$. أيضا، من ذلك نستنتج أن M تحوى أعدادا صحيحة موجبة. وعندئذ تحتوي M على أصغر عدد صحيح موجب وليكن c . وحيث إن $c\in M$ ، فإن c تأخذ الصيغة $c=m_0a+n_0b$. إننا ندعي الآن أن $c=(a,b)$. لبرهان هذا الادعاء، نلاحظ أولا، أنه إذا كان $d|a$ و $d|b$ فإن $d|m_0a+n_0b$ ومن ثم فإن $d|c$. والآن نثبت أن $c|a$ و $c|b$. لنفرض أن $x=ma+nb$ عنصر من M . استنادا إلى الخوارزم الإقليدي نجد أن $x=tc+r$ حيث $0\leq r<c$. بالتعويض عن x,c نحصل على

$$ma + nb = t\,(m_0a + n_0b) + r$$

وبالتالي فإن

$$r = (m-tm_0)a + (m-tn_0)\,b$$

وهذا يقتضي أن $r\in M$. ولما كان $r<c$ و $0\leq r$ وحيث إن c هو أصغر عدد صحيح موجب في M ، لذلك نستنتج أن $r=0$ وبالتالي $x=tc$ مما يثبت أن $c|x$ لأي عنصر x في M ، ولكن $a=1.a+0.b\in M$ و $b=0.a+1.b\in M$ ولذلك يكون $c|b$ و $c|a$. وهكذا نكون قد برهنا على أن العدد c يحقق شرطي تعريف القاسم المشترك الأعظم بالنسبة للعددين b,a ، أي أن $c=(a,b)$. وبذلك يتم برهان التمهيدية.

تعريف

يقال إن العددين الصحيحين b,a ***أوليان نسبيا*** *(Relatively primes) إذا كان $(a,b)=1$.*

وكنتيجة مباشرة للتمهيدية (١-٣-١) لدينا ما يلي.

نتيجة

إذا كان b,a أوليين نسبيا فإنه يوجد عددان صحيحان n,m بحيث يكون $ma+nb=1$.

الآن نناقش فكرة أخرى مألوفة هي فكرة العدد الأولي والتي نعني بها العدد الصحيح الذي ليس له تحليل غير تافه. وسوف نستبعد الواحد الصحيح من مجموعة الأعداد الأولية لأسباب فنية.

إن المتتالية ....2,3,5,7,11 هي أعداد أولية. وبالمثل فإن ,....,5-,3-,2- أعداد أولية.

ولما كان العدد السالب لا يقود إلى فروق جوهرية، عند التحليل، لذا فإن الأعداد الأولية ستعني بالنسبة لنا الأعداد الأولية الموجبة.

تعريف

يقال إن العدد p حيث $p>1$ ***عدد أولي*** *(Prime number) إذا كانت* ***قواسمه*** *الوحيدة هي ± 1 , $\pm p$.*

وبعبارة أخرى يكون العدد الصحيح $p(p>1)$ عددا أوليا إذا وفقط إذا كان $(p,n)=1$ أو $p|n$ ، لأي عدد صحيح n . سنرى بعد قليل أن الأعداد الأولية تمثل حجر الزاوية للأعداد الصحيحة.

تمهيدية (١-٣-٢)

إذا كان العدد a أوليا بالنسبة للعدد b وكان $a|bc$ فإن $a|c$.

البرهان

لما كان b,a أوليين نسبيا فإنه وفقا لنتيجة التمهيدية (١-٣-١) نستطيع الحصول على عددين صحيحين n,m بحيث يكون $ma+nb=1$. وعندئذ، $mac+nbc=c$ ، ومن الواضح أن $a|mac$ ومن الفرض $a|nbc$ ، وبالتالي $a|(mac+mbc)$. ولما كان $mac+nbc=c$ ، فإننا نستنتج أن $a|c$ وهذا هو المطلوب إثباته في التمهيدية.

ونستنتج من تعريف العدد الأولي والتمهيدية (١-٣-٢) النتيجة المهمة الآتية.

نتيجة

إذا كان عدد أولي يقسم حاصل ضرب أعداد صحيحة فإنه يجب أن يقسم واحدًا من هذه الأعداد على الأقل.

إن برهان هذه النتيجة متروك للقارىء.

لقد أكدنا على أن الأعداد الأولية هي اللبنات الأساسية لمجموعة الأعداد الصحيحة. إن التعبير الدقيق عن هذه الحقيقة، المهمة، يكمن في مبرهنة التحليل الوحيد.

مبرهنة (١-٣-١)

إن أي عدد صحيح موجب $a>1,a$ يمكن تحليله بطريقة وحيدة على الصيغة

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ldots\ldots p_t^{\alpha_t}$$

حيث $p_1>p_2>\ldots\ldots>p_t$ *هي أعداد أولية و* $\alpha_i>0$.

البرهان

إن المبرهنة، في الواقع، كما وردت تتكون من مبرهنتين جزئيتين مختلفتين. أولاهما إمكانية تحليل العدد الصحيح المعطى إلى حاصل ضرب قوي أعداد أولية والثانية تؤكد أن هذا التحليل وحيد. لذلك فإن إثبات هذه المبرهنة يتم بإثبات كل من هاتين المبرهنتين الجزئيتين بصورة منفصلة.

إن السؤال الذي يطرح نفسه هو: كيف نبدأ إثبات هذه المبرهنة؟ . . .

إن الطريقة الطبيعية للبدء بالبرهان هو استخدام مبدأ الاستقراء الرياضي. حيث سنستخدم الصيغة الآتية لهذا المبدأ؛ إذا كانت القضية $p(m_0)$ صحيحة وإذا

كانت صحة القضايا $p(r)$ لجميع قيم r التي تحقق الشرط $m_0 \leq r < k$ تقتضي صحة القضية $p(k)$ فإن $p(n)$ صحيحة لجميع قيم n بحيث $n \geq m_0$.

إنه يمكن إثبات أن هذه الصيغة لمبدأ الاستقراء الرياضي ليست إلا نتيجة للخاصة الأساسية لمجموعة الأعداد الصحيحة التي تنص على أن أية مجموعة غير خالية من الأعداد الصحيحة الموجبة تحوى عنصرا أصغر. (انظر مسألة ١٠).

سنثبت أولا أن كل عدد صحيح a حيث $a>1$ يمكن تحليله إلى حاصل ضرب قوى أعداد أولية وسيكون منطلقنا في البرهان هو الاستقراء الرياضي. حيث إن العدد $m_0=2$ عدد أولي، لذلك فإنه يمكن كتابته على هيئة قوى عدد أولي.

لنفرض الآن أنه يمكن تحليل أي عدد صحيح r حيث $2 \leq r < k$ إلى حاصل ضرب قوى أعداد أولية. فإذا كان k نفسه عددا أوليا، فإنه يمكن كتابته كحاصل ضرب قوى أعداد أولية. أما إذا كان k ليس عددا أوليا، فإنه يمكن كتابته على الصيغة $k=uv$ حيث $1<u<k$ و $1<v<k$. ومن فرضية الاستقراء الرياضي لما كان كل من v,u أقل من k ، لذلك يمكن تحليل كل منهما إلى حاصل ضرب قوى أعداد أولية ووفقا لذلك، فإن $k=uv$ يمكن تحليله إلى حاصل ضرب قوى أعداد أولية. لقد أثبتنا أن صحة القضية لجميع الأعداد الصحيحة r حيث $2 \leq r < k$ تقتضي صحتها للعدد k نفسه. وبالتالي ومن مبدأ الاستقراء الأساسي فإن القضية صحيحة لجميع الأعداد الصحيحة n حيث $n \geq m_0 = 2$ مما يعني أن أي عدد صحيح n حيث $n \geq 2$ هو حاصل ضرب قوى أعداد أولية.

لإثبات وحدانية التحليل نستخدم مرة أخرى مبدأ الاستقراء الرياضي. بالطريقة نفسها المستخدمة سابقا، لنفرض أن:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_s^{\beta_s}$$

حيث $p_1>p_2>......>p_r$ و $q_1>q_2>.....>q_s$ ، أعــداد أولية كما أنـه $\alpha_i>0$ و $\beta_i>0$ لكل i :

إن هدفنا هو برهان أن :

(١) $r=s$

(٢) $p_1=q_1, p_2=q_2, ..., p_r=q_r$

(٣) $\alpha_1=\beta_1, \alpha_2=\beta_2, ..., \alpha_r=\beta_r$

إن من الواضح صحة النظرية عندما $a=2$.

لنفرض الآن صحة النظرية لجميع الأعداد الصحيحة u حيث $2\leq u<a$

الآن، بما أن

$$a=p_1^{\alpha_1}....p_r^{\alpha_r}=q_1^{\beta_1}....q_s^{\beta_s}$$

وبما أن $\alpha_1>0$ و $p_1|a$ ، لذلك فإن $p_1|q_1^{\beta_1}....q_s^{\beta_s}$ ومع ذلك، لما كان p_1 عددا أوليا فإنه من نتيجة التمهيدية (١-٣-٢) نجد بسهولة أن $p_1=q_i$ ، لإحدى قيم i . وهكذا فإن $p_1=q_i\leqslant q_1$ وبالمثل، لما كان $q_1|a$ ، فإننا نجد $q_1=p_j$ لإحدى قيم j ومن ثم فإن $q_1=p_j\leqslant p_1$. وهكذا نكون قد أثبتنا أن $p_1=q_1$ وبالتالي فإن

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}=p_1^{\beta_1}q_2^{\beta_2}\dots q_s^{\beta_s}$$

إننا ندعي أن هذا يقتضي أن $\alpha_1=\beta_1$ (أثبت ذلك!)

ولكن عندئذ

$$b=\frac{a}{p_1^{\alpha_1}}=p_2^{\alpha_2}\dots p_r^{\alpha_r}=q_2^{\beta_2}\dots q_s^{\beta_s}$$

فإذا كانت $b=1$ فإن $\alpha_2=...=\alpha_r=0$ و $\beta_2=...=\beta_s=0$ مما يعني أن $r=s=1$.
الآن إذا كانت $b>1$ ونظرا لكون $b<a$ فإمكاننا تطبيق فرضية الاستقراء الرياضي على العدد b لنحصل على:

(١) عدد العوامل ذات القوى الأولية المختلفة للعدد b متساو في كلا الجانبين، أي أن $r-1=s-1$ ، مما يعني أن $r=s$.

(٢) $\alpha_2 = \beta_2 ,\ldots, \alpha_r = \beta_r$

(٣) $p_2 = q_2 ,\ldots, p_r = q_r$

بهذه المعلومات مع ما حصلنا عليه آنفا، أي، $\alpha_1=\beta_1, p_1=q_1$ نكون قد أنهينا تماما المطلوب إثباته. وهكذا نرى أن افتراض وحدانية التحليل للأعداد الصحيحة التي هي أقل من a تقتضي وحدانية التحليل للعدد الصحيح a نفسه. وعليه فإن برهان التحليل الوحيد بواسطة الاستقراء الرياضي قد انتهى.

نتجه الآن نحو دراسة فكرة مهمة هي التطابق قياس عدد صحيح مفروض. وكما سنرى لاحقا فإن العلاقة التي سنقدمها الآن ليست إلا حالة خاصة من علاقة أكثر شمولا والتي يمكن أن تعرف في سياق أعم.

تعريف

ليكن n ، حيث $n>o$ عددًا صحيحًا . نقول إن a يطابق b قياس n ونكتب $a\equiv b \bmod n$ إذا كان $n|(a-b)$.

يطلق على هذه العلاقة «**التطابق قياس n**» (Congruence modulo n) كما يطلق على العدد n «**مقياس**» (modulus) هذه العلاقة. لاحظ، على سبيل المثال، أن $73\equiv 4 \bmod 23$ وأن $21\equiv -9 \bmod 10$ وهكذا . . .

إن علاقة التطابق هذه تتمتعُ بالخواص الآتية:

تمهيدية (١-٣-٣)

(١) علاقة التطابق قياس n تعرف علاقة تكافؤ على مجموعة الأعداد الصحيحة .

(٢) عدد فصول تكافؤ هذه العلاقة يساوي n .

(٣) *إذا كان $a\equiv b \bmod n$ و $c\equiv d \bmod n$ فإن*
$a+c\equiv (b+d) \bmod n$ و $ac\equiv bd \bmod n$.

(٤) *إذا كان $ab\equiv ac \bmod n$ وكان a أوليا بالنسبة إلى n*
فإن $b\equiv c \bmod n$.

البرهان

سنثبت أولا أن علاقة التطابق قياس n هي علاقة تكافؤ.

بما أن $n|0$ ، لذلك نجد أن $n|a-a$ وهذا يقتضي أن $a\equiv a \bmod n$ ، لكل عدد صحيح a . كذلك إذا كان $a\equiv b \bmod n$ فإن $n|(a-b)$. وبالتالي $n|b-a$ ، لأن $b-a=-(a-b)$. أي أن $b\equiv a \bmod n$

وأخيرا إذا كان $a\equiv b \bmod n$ و $b\equiv c \bmod n$ فإن $n|a-b$ و $n|b-c$ وبالتالي $n|\{(a-b)+(b-c)\}$ أي أن، $n|a-c$ ، وعليه فإن $a\equiv c \bmod n$.

لنرمز إلى فصل تكافؤ العنصر a بالنسبة لهذه العلاقة بالرمز $[a]$ ونسمي فصل التكافؤ هذا بـ**فصل التطابق** للعنصر a (قياس n) . فإذا كان a أي عدد صحيح ، فإنه باستخدام الخوارزم الإقليدي نجد أن $a=kn+r$ حيث $0\leq r<n$ ولكن عندئذ نجد أن $a\in[r]$ ، وبـالتالي $[a]=[r]$. وهكذا فإنه يوجد على الأكثر فصول تطابق عددها n ، وبالإضافة إلى ذلك، فإن هذه الفصول مختلفة لأنه إذا كان $[i]=[j]$ ، حيث $0\leq i<j<n$ ، على سبيل الافـتراض، فإن $n|(j-i)$ حيث $j-i$ عدد صحيح موجب أقـل من n ومن الواضح أن هذا مستحيل، وبالتالي فإنه يوجد فصول تطابق مختلفة عددها هو n تماما وهي $[0], [1],\ldots,[n-1]$. وهكذا نكون قد برهنا الجزئين الأول والثاني من التمهيدية .

والآن إلى الجزء الثالث من التمهيدية .

لنفرض أن $a\equiv b(\bmod n)$ وأن $c\equiv d \bmod n$ عندئذ، $n|(a-b)$, $n|(c-d)$
وبالتالي $n|(a-b)+(c-d)$ أي ، $n|(a+c)-(b+d)$ ولكن عندئذ، $a+c\equiv b+d \bmod n$.
وبالاضافة إلى ذلك $n|(a-b)c+(c-d)b$ ، وحيث إن $(a-b)c+(c-d)b=ac-bd$ لذلك نجد

أن : $n|(ac-bd)$ أي أن $ac \equiv bd \bmod n$ وأخيرا نلاحظ أنه إذا كان $ab \equiv ac \bmod n$ وكان a أوليا بالنسبة إلى n ، فإنه استنادا إلى أن $n|a(b-c)$ واستنادا إلى التمهيدية (١-٣-٢) فإن هذا يقتضي أن $n|(b-c)$ ومن ثم فإن $b \equiv c \bmod n$.

نلاحظ أن الجزء الرابع من هذه التمهيدية قد لا يكون صحيحا وذلك عندما يكون a ليس أوليا بالنسبة إلى n .

فعلى سبيل المثال

$2.3 \equiv 4.3 \bmod 6$ ، على الرغم من أن $2 \not\equiv 4 \bmod 6$

إن التمهيدية (١-٣-٣) تمهد الطريق لمعلومات ممتعة من وجهة نظرنا.

لنفرض أن Z_n هي مجموعة فصول التطابق قياس n أي أن،

$.Z_n = \{[0], [1], \ldots, [n-1]\}$

فإذا كان $[i], [j] \in Z_n$

وعرفنا

$$[i] + [j] = [i + j] \qquad \text{(a)}$$

$$[i]\,[j] = [i\,j] \qquad \text{(b)}$$

فإن التمهيدية (١-٣-٣) تضمن لنا أن هاتين العمليتين، أي «الجمع» و«الضرب» حسنتا التعريف، بمعنى أنه إذا كان :

$$[j] = [j'] \,,\, [i] = [i']$$

فإن

$$[i] + [j] = [i + j] = [i' + j'] = [i'] + [j']$$

وأن،

$$[i]\,[j] = [i']\,[j']$$

(تحقق من ذلك).

إن لهاتين العمليتين على Z_n الخواص الآتية (والتي سنترك براهينها كتمارين).

لأي ثلاثة عناصر $[k], [j], [i]$ في Z_n يكون لدينا :

(١) $[i]+[j]=[j]+[i]$ } قانوني الابدالية
(٢) $[i][j]=[j][i]$

(٣) $([i]+[j])+[k]=[i]+([j]+[k])$ } قانوني التجميع
(٤) $([i][j])[k]=[i]([j][k])$

(٥) $[i]([j]+[k])=[i][j]+[i][k]$ (قانون التوزيع)

(٦) $[0]+[i]=[i]$

(٧) $[1][i]=[i]$

ملاحظة أخرى، هي أنه إذا كان $n=p$ حيث p عدد أولي، وكان $[a]\neq[0]$ عنصرا من Z_n ، فإنه يوجد عنصر $[b]$ من Z_n بحيث يكون $[a][b]=[1]$.

إن المجموعة Z_n تلعب دورا بالغ الأهمية في الجبر ونظرية الأعداد ويطلق عليها **مجموعة الأعداد الصحيحة قياس** n (Integers mod n) . وبهذا نكون قد ألممنا بها قبل أن نمضي قدما في دراستنا.

مسائل

١ - إذا كان $a|b$ و $b|a$ فأثبت أن $a=\pm b$.

٢ - إذا كان b قاسما للعددين h,g فأثبت أنه قاسم للعدد $mg+nh$.

٣ - إذا كان b,a عددين صحيحين فإننا نعرف **المضاعف المشترك الأصغر** (least common multiple) لهما والذي نرمز له بالرمز $[a,b]$ بأنه ذلك العدد الصحيح الموجب d بحيث يكون

ا) $a|d$ و $b|d$.

ب) إذا كان $a|x$ و $b|x$ فإن $d=x$.

برهن على وجود $[a,b]$ وأنه إذا كان $a>0$, $b>0$ فإن :

$$[a,b]=\frac{ab}{(a,b)}$$

٤ ـ إذا كان $a|x$ و $b|x$ وكان $(a,b)=1$ فأثبت أن $(a\,b)|x$.

٥ ـ إذا كان $b = p_1^{\beta_1} \dots p_k^{\beta_k}\ ,\ a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

حيث p_i أعداد أولية مختلفة و $\beta_i \geqslant 0\ ,\ \alpha_i \geqslant 0$ فأثبت أن

(ا) $(a,b) = p_1^{\delta_1} \dots p_k^{\delta_k}$

حيث δ_i هو أصغر العددين α_i و β_i لكل i .

(ب) $[a,b] = p_1^{\gamma_1} \dots p_k^{\gamma_k}$

حيث γ_i هو أعظم العددين α_i و β_i لكل i .

٦ ـ ليكن b,a عددين ؛ بتطبيق الخوارزم الإقليدي على التتابع يكون لدينا :

$$a = q_0 b + r_1 \qquad 0 \leqslant r_1 < |b|$$

$$b = q_1 r_1 + r_2 \qquad 0 \leqslant r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3 \qquad 0 \leqslant r_3 < r_2$$

. . .

. . .

. . .

$$r_k = q_{k+1} r_{k+1} + r_{k+2} \qquad 0 \leqslant r_{k+2} < r_{k+1}$$

وحيث إن الأعداد الصحيحة r_k متناقصة كما أنها غير سالبة ، لذا فإنه يوجد أول عدد صحيح n بحيث يكون $r_{n+1} = 0$ أثبت أن $r_n = (a,b)$ (اعتبر هنا أن $r_0 = |b|$)

٧ ـ باستخدام المسألة السابقة ، احسب ما يلي :

(ا) $(1128,33)$ (ب) $(6540, 1206)$

٨ ـ لتقرير ما إذا كان n عددا أوليا أثبت أنه يكفي أن نبرهن أنه غير قابل للقسمة على أي عدد أولي p بحيث يكون $p \leqslant \sqrt{n}$

٩ ـ أثبت أن العدد n حيث $n>1$ يكون أوليا إذا وفقط إذا كان لأي عدد a إمَّا أن يكون $(a,n)=1$ أو $n|a$.

١٠ ـ على افتراض وجود عنصر أصغر في أية مجموعة غير خالية من الأعداد الصحيحة الموجبة ،

ا) لنفرض أن p قضية وأن

١) $p(m_0)$ صائبة .

٢) صواب $p(m-1)$ يقتضي صواب $p(m)$.

أثبت أن $p(n)$ صائبة لأي عدد n حيث $n \geqslant m_0$

ب) إذا كانت القضية p تحقق .

١) $p(m_0)$ صائبة .

٢) متى ما كانت $p(a)$ صائبة لجميع الأعداد a حيث $m_0 \leqslant a < m$ فإن $p(m)$ صائبة .

فأثبت أن $p(n)$ صائبة لأي عدد n حيث $n \geqslant m_0$

١١ - برهن على أن عمليتي الجمع والضرب على المجموعة Z_n حسنتا التعريف .

١٢ - برهن الخواص من ١-٧ لعمليتي الجمع والضرب على Z_n .

١٣ - إذا كان $(a,n) = 1$ فإنه يوجد $[b] \in Z_n$ بحيث يكون $[a][b] = [1]$

١٤ - إذا كان p عددا أوليا فأثبت أنه لأي عدد صحيح a يكون $a^p \equiv a \bmod p$.

١٥ - إذا كان $(m,n)=1$ وكان لدينا العددان b,a فأثبت : أنه يوجد عدد x بحيث يكون $x \equiv a \bmod m$ و $x \equiv b \bmod n$.

١٦ - برهن نتيجة التمهيدية (١-٣-٢) .

١٧ - أثبت أن العدد n يكون أوليا إذا وفقط إذا كان $[a][b]=[0]$ في Z_n فإن هذا يقتضي أن يكون $[a] = [b] = [0]$.

قراءات إضافية في المجموعات والأعداد الرئيسة

Birkhoff, G. and MacLane, S. *A Brief Survey of Modren Algebra,* 2nd Ed. New York: The Macmillan Company, 1965.

٢

نظرية الزمر

● تعريف الزمرة ● أمثلة على الزمر ● بعض التمهيديات الأولية ● الزمر الجزئية ● أحد مبادىء العدّ ● الزمر الجزئية الناظمية والزمر الخارجة ● التشاكلات ● التماثلات الذاتية ● مبرهنة كيلي ● زمر التبديلات ● مبدأ آخر للعدّ ● مبرهنة سيلو ● الضرب المباشر ● الزمر الابدالية المنتهية

سوف نباشر في هذا الفصل دراسة البنية الجبرية المعروفة **بالزُمْرَةْ**، والتي هي لبنة أساسية في موضوع يدعى اليوم **بالجبر المجرد**. وفي فصول لاحقة سنلقي نظرة على مواضيع أخرى مثل الحلقات، الحقول، فضاءات المتجهات، الجبر الخطي، وعلاوة على العرف المتبع بالبدء بالزمرة، فهناك أسباب تبرر هذا الاختيار من بينها، أن الزمر هي أنظمة ذات عملية واحدة مما تجعل دراستها أمرا بسيطا، ولكن رغم هذه البساطة، فإن المفاهيم الجبرية الأساسية مثل التشاكلات والبنى الخارجة وما شابه ذلك، والتي تلعب دورًا بارزًا في البنى الجبرية، بل وفي الحقيقة، في جميع فروع الرياضيات تدخل هنا ـ من الآن ـ بصورة نقية وواضحة.

وهنا وقبل أن نبدأ بالتفاصيل، دعنا نلقي نظرة سريعة إلى ما سيأتي. إننا نجد في الجبر المجرد أنظمة أساسية معيّنة اكتسبت مواقع ذات أهمية عظمى في تاريخ تطور الرياضيات. هذه الأنظمة هي عبارة عن مجموعات يمكن أن نتعامل جبريا مع

عناصرها، ونعني بذلك أننا نستطيع أن نركّب عنصرين في المجموعة، وربما بعدة طرق، كي نحصل على عنصر ثالث من هذه المجموعة. كما نفترض، بالإضافة إلى ذلك، أن هذه العمليات الجبرية تخضع لقوانين محددة، والتي هي موضحة بصراحة بما نسميه بالمسلمات أو الفرضيات المعرفة للنظام.

وعندئذ، في هذا الوضع المجرد نحاول برهنة نظريات متعلقة بهذه البنى العامة آملين دائما أنه عندما نطبق هذه النتائج على حالة خاصة فإنها ستضفي على هذه الحالة التي في متناول أيدينا وضوحا لجوانب قد تخفى عند تناولنا دراستها من وجهة نظر خاصة، ذلك لأننا، عندئذ، قد نكون مهتمين بتفاصيل قد لا تمت لموضوع الدراسة بصلة.

ونحب أن نؤكد أن للأنظمة الجبرية والموضوعات التي تعرفها طابعا مألوفا، وأنها يجب أن تنبثق من خبرتنا بأمثلة متعددة كما أنها يجب أن تكون غنية بنتائج مفيدة. إنه لا يمكن لأي إنسان أن يسرد مسلمات قليلة ثم يستأنف دراسة الأنظمة الموصوفة على أساسها وهذا، صراحة، هو ما يفعله البعض، ولكن معظم الرياضيين يعتبرون هذه المحاولات رياضيات غير مفيدة.

إن سبب اختيارنا أنظمة للدراسة هو كونها حالة خاصة من بُنَى ظهرت مرة بعد مرة حيث لاحظ بعض الرياضيين أخيرا أن هذه الحالات الخاصة كانت بالفعل أمثلة خاصة لظاهرة عامة وكذلك وجود تشابه بين موضوعين رياضيين مختلفين تماما ومن ثم قاد هذا إلى البحث عن أسباب هذا التشابه. وثمة مثال على هذه الظاهرة هو النظام الذي نعرفه اليوم بالزمرة، والذي بدأت دراسته في نهاية القرن الثامن عشر وبداية القرن التاسع عشر، ولكنه لم يُقَدّم بالشكل الذي هو عليه اليوم إلا في نهاية القرن التاسع عشر. إن البنى الجبرية التي ندرسها في الوقت الحاضر هي تلك التي أُسست على قواعد متينة من دراسة حالات خاصة، وبقيت رغم مرور الزمن نظرا لأهميتها، ولذلك فلا يوجد شك من أحد من الرياضيين في أهمية الموضوع الأول الذي اخترناه للدراسة وهو موضوع الزمر.

(٢ ـ ١) تعريف الزمرة

من المستحسن أن نعيد إلى الذاكرة هنا ما نوقش في الفصل الأول. لقد عرفنا المجموعة $A(S)$ بأنها **مجموعة التطبيقات الأحادية** من المجموعة S على نفسها، حيث S أية مجموعة غير خالية. كذلك تعرفنا على حاصر ضرب التطبيقين σ و τ من $A(S)$ ورمزنا له بالرمز $\sigma\circ\tau$. كذلك يتضح مما سبقت دراسته في الفصل الأول أن عناصر $A(S)$ قد حققت الخواص الآتية بالنسبة لحاصل الضرب هذا:

١) لأي عنصرين σ و τ في $A(S)$ يكون $\sigma\circ\tau$ عنصرا في $A(S)$ (ويمكن وصف هذا بقولنا إن $A(S)$ **مغلقة** (closed) بالنسبة لعملية الضرب).

٢) لأي ثلاثة عناصر σ و τ و μ في $A(S)$ يكون $(\sigma\circ\tau)\circ\mu = \sigma\circ(\tau\circ\mu)$ وتدعى هذه العلاقة **بالقانون التجميعي** (Associative law) .

٣) يوجد عنصر خاص i في $A(S)$ يحقق العلاقة $i\circ\sigma=\sigma\circ i=\sigma$ لكل σ في $A(S)$ ومثل هذا العنصر يدعى **بالعنصر المحايد** (Identity element) .

٤) لكل عنصر $\sigma\in A(S)$ يوجد عنصر في $A(S)$ يرمز له بالرمز σ^{-1} بحيث إن $\sigma\circ\sigma^{-1} = \sigma^{-1}\circ\sigma = i$. ويمكن وصف هذا بقولنا إنه يوجد لكل عنصر في $A(S)$ **معكوس** (Inverse) في $A(S)$.

بقيت حقيقة أخرى، حول $A(S)$ ، هي أنه إذا كانت S تحتوي على ثلاثة عناصر فأكثر فإنه يمكننا إيجاد عنصرين $\alpha, \beta\in A(S)$ بحيث يكون $\alpha\circ\beta\neq\beta\circ\alpha$. إن هذه الحقيقة التي تخالف ما عهدناه سابقا في الرياضيات تجعل $A(S)$ تتمتع بصفة لم تقابلنا من قبل في غيرها.

بهذا المثال، كنموذج، نأتي إلى التعريف الآتي:

تعريف

يقال عن مجموعة غير خالية G إنها زمرة (group) إذا كانت توجد عملية ثنائية معرفة على G تدعى حاصل الضرب ويرمز لها بالرمز "." بحيث تتحقق الشروط التالية:

١) *إذا كان* $a,b \in G$ *فإن* $a.b \in G$ ***(الإغلاق)***.

٢) ***إذا كان*** $a,b,c \in G$ ***فإن*** $(a.b).c=a.(b.c)$ ***(قانون التجميع)***

٣) يوجد عنصر e في G بحيث يكون $a.e = e.a = a$ لكل $a \in G$ ***(وجود العنصر المحايد e في G)***

٤) *لكل عنصر* a *في* G *يوجد عنصر* a^{-1} *في* G *بحيث يكون* $a.a^{-1}=a^{-1}.a=e$ ***(وجود معكوس لكل عنصر في G)***

وبالرجوع إلى مصدر هذا التعريف نجد أنه ليس غريبا أنه لأية مجموعة غير خالية S تكون المجموعة A(S) زمرة. وهكذا فإننا قد وجدنا مصدرا غير محدود من الزمر الملموسة والمشوقة. وسنرى فيما بعد (في مبرهنة تنسب إلى كايلي (Cayley)) أن الزمر A(S) تُكوِّن عائلة عامة من الزمر. وإذا كانت S تحتوي على ثلاثة عناصر أو أكثر، فإننا نعيد إلى الذاكرة أنه بالإمكان إيجاد عنصرين $\sigma\, \tau \in A(S)$ بحيث يكون $\sigma \circ \tau \neq \tau \circ \sigma$ وهذا يحثنا على أن نفرد نوعا خاصا، ولكنه بالغ الأهمية، من الزمر كما في التعريف التالي:

تعريف

*يقال عن الزمر G إنها زمرة **إبدالية أو آبلية** (Abelian or Commutative) إذا كان* $a.b=b.a$ *لكل* $a,b \in G$.

إن الزمرة التي ليست إبدالية تدعى، بالطبع، غير إبدالية. وحيث إننا قد رأينا أمثلة من هذه الزمرة، لهذا نعلم أن الزمرة غير الإبدالية موجودة بالفعل.

إن عدد العناصر التي تحتوي عليها الزمرة G هو مميز آخر للزمرة وسنطلق عليه **رتبة** الزمرة G (Order of G) ، ونرمز له بالرمز **o(G)** .

إن هذا العدد يكون أكثر أهمية عندما يكون منتهيا وفي تلك الحالة نطلق على الزمرة G **الزمرة المنتهية** (Finite group). إن الزمرة المنتهية غير التافهة موجودة. لكي

نرى ذلك يكفي أن نلاحظ أنه إذا كانت S مجموعة تحتوي على n من العناصر فإن الزمرة A(S) تحتوي على !n من العناصر. (أثبت ذلك).

إن هذا المثال ذا الأهمية البالغة يرمز له بالرمز S_n في كل ما سيأتي في هذا الكتاب وسيدعى **بزمـرة التناظر** (Symmetric group) من الدرجة n وفي البند الآتي سندرس بعناية S_3 والتي هي زمرة غير إبدالية رتبتها 6 .

(٢ - ٢) أمثلة على الزمر

مثال (٢-٢-١)

لتكن G مجموعة الأعداد الصحيحة $0, \pm1, \pm2, \ldots$ حيث نعني بالعملية a.b لكل $a,b \in G$ عملية جمع الأعداد الصحيحة العادية، أي أن $a.b=a+b$.

إن باستطاعة القارىء أن يتأكد وبسهولة أن G هي زمرة إبدالية غير منتهية حيث يلعب العنصر 0 دور العنصر المحايد و $-a$ هو معكوس العنصر a .

مثال (٢-٢-٢)

لتكن G هي المجموعة التي تتكون من العددين الحقيقيين 1 و -1 . عندئذ تكون G زمرة إبدالية رتبتها 2 بالنسبة لعملية ضرب الأعداد الحقيقية.

مثال (٢-٢-٣)

لتكن $G=S_3$ ، أي زمرة جميع التطبيقات الأحادية من المجموعة $\{x_1, x_2, x_3\}$ على نفسها. عندئذ فإن G زمرة رتبتها 6 بالنسبة لعملية تركيب التطبيقات التي عرفناها في الفصل الأول. الآن نحيد قليلا وذلك قبل الاستمرار في هذا المثال.

من أجل ترميز أدق، ليس فقط في S_3 ، بل في أية زمرة، دعنا نعرف ما يلي لأي عنصر $a \in G$.

$$a^0 = e\ ,\ a^1 = a\ ,\ a^2 = a.a\ ,\ a^3 = a.a^2, \ldots,\ \ a^k = a.a^{k-1}$$

و

$$a^{-2} = (a^{-1})^2\ ,\ a^{-3} = (a^{-1})^3\ , \ldots,\ etc$$

ويمكن للقارىء التأكد من أن قوانين الأسس، سارية المفعول هنا، وبعبارة أخرى، لأي عددين صحيحين n,m (موجبين أو سالبين أو صفرًا) يكون:

$$a^m.a^n = a^{m+n} \tag{1}$$

$$(a^m)^n = a^{mn} \tag{2}$$

(تجدر الإشارة هنا إلى أنه إذا كانت G هي الزمرة الواردة في المثال (٢ـ٢ـ١) فإن a^n يعني na).

دعنا الآن نعود إلى مثالنا S_3 ونفحصه عن كثب، مع وضع هذه الملاحظة نصب أعيننا. لنعتبر التطبيق ϕ المعرف على المجموعة x_1, x_2, x_3 كما يلي:

$$\phi: \quad \begin{array}{l} x_1 \to x_2 \\ x_2 \to x_1 \\ x_3 \to x_3 \end{array}$$

ولنعتبر كذلك التطبيق

$$\psi: \quad \begin{array}{l} x_1 \to x_2 \\ x_2 \to x_3 \\ x_3 \to x_1 \end{array}$$

إنه، بالتحقق، نرى وبسهولة أن:

$$\phi^2 = e, \quad \psi^3 = e$$

وأن

$$\phi.\psi: \quad \begin{array}{l} x_1 \to x_3 \\ x_2 \to x_2 \\ x_3 \to x_1 \end{array}$$

بينما

$$\psi.\phi: \quad \begin{array}{l} x_1 \to x_1 \\ x_2 \to x_3 \\ x_3 \to x_2 \end{array}$$

إن من الـواضح أن $\psi.\phi \neq \phi.\psi$ وذلك لأنهما لا ينقلان x_1 إلى الصورة نفسها. ولما كان $\psi^3 = e$ ، لذا فإنه ينتج أن $\psi^{-1} = \psi^2$. والآن دعنا نرى تأثير $\phi.\psi^{-1}$ على x_1 و x_2 و x_3.
لما كان $\psi^{-1} = \psi^2$ و كان

$$\psi^2: \quad \begin{array}{l} x_1 \to x_3 \\ x_2 \to x_1 \\ x_3 \to x_2 \end{array}$$

فإنه يكون لدينا

$$\psi^{-1}.\phi: \quad \begin{array}{l} x_1 \to x_3 \\ x_2 \to x_2 \\ x_3 \to x_1 \end{array}$$

وبعبـارة أخـرى $\phi.\psi = \psi.^{-1}\phi$. لنعتبر العناصر $e, \phi, \psi, \psi^2, \phi.\psi, \psi.\phi$ ، إن هذه العناصر جميعها مختلفة وتنتمي إلى G (لأن G مغلقة) التي تحتوي على 6 عناصر فقط. وعليه فإن هذه القائمة تضم جميع عناصر G . وربما يسأل إنسان، على سبيل المثال، ما هو العنصر الـذي يقـابـل $\psi(\phi.\psi)$ في هذه القـائمـة؟ والجواب على ذلك هو أنه باستخدام العلاقة $\phi.\psi = \psi.^{-1}\phi$ نجد أن

$$\psi.(\phi.\psi) = \psi.(\psi^{-1}.\phi) = (\psi.\psi^{-1})\,\phi = e.\phi = \phi$$

وثمة عبارة أخرى ذات أهمية هي العبارة:

$$(\phi.\psi).(\psi.\phi) = \phi(\psi.(\psi.\phi)) = \phi.(\psi^2.\phi) = \phi.(\psi^{-1}\phi) = \phi.(\phi.\psi) = \phi^2.\psi = e.\psi = \psi$$

(لا ينبغي، للقـاريء هنـا أن يتخـوف من هذه السلسلة المملة والطويلة من المتساويات. إنها ستكون المرة الأخيرة التي نتطرق بها إلى مثل هذه الأمور). وباستخدام الطريقة نفسها، كالتي رأينا، يستطيع القاريء أن يحسب حواصل الضرب الخمسة والعشرين، والتي لا تشمل العنصر المحايد e ، والتي سيرد بعضا منها في المسائل.

مثال (٢-٢-٤)

لنفرض أن n هو أي عدد صحيح، سنكون الآن زمرة رتبتها n كما يلي: إن G تتكون من جميع الرموز a^i و $i=0,1,2,...n-1$، حيث نفرض أن $a^0=a^n=e$ و $a^i \cdot a^j=a^{i+j}$ إذا كان $i+j\leqslant n$ و $a^i.a^j=a^{i+j-n}$ إذا كان $i+j>n$.

يمكن للقارىء التأكد من أن هذه زمرة. وهذه الزمرة يطلق عليها **الزمرة الدورية** (Cyclic group) من الرتبة n إن التفسير الهندسي للزمرة الواردة في المثال (٢-٢-٤) هو كما يلي:

لتكن S دائرة في المستوى نصف قطرها الواحد الصحيح، وأن ϱ_n هو الدوران بزاوية قدرها $\frac{2\pi}{n}$، عندئذ $\varrho_n \in A(S)$، كذلك فإن ϱ_n يوّلد زمرة رتبتها n عناصرها هي:

$$\{e, \varrho_n, \varrho_n^2, \ldots, \varrho_n^{n-1}\}$$

مثال (٢-٢-٥)

لتكن S هي مجموعة الأعداد الصحيحة، كالمعتاد، لنفرض أن A(S) هي مجموعة التطبيقات الأحادية من S على نفسها.

كذلك، لتكن G هي مجموعة كل العناصر في A(S) التي تحرك عددا **منتهيا فقط** من عناصر S، بعبارة أخرى، $\sigma \in G$ إذا وفقط إذا كانت المجموعة $\{x\in S:x\sigma\neq x\}$ منتهية. ليكن $\sigma.\tau$ هو حاصل ضرب العنصرين τ,σ في G اللذين ينتميان بطبيعة الحال إلى A(S). إننا ندعي أن G زمرة بالنسبة لهذه العملية.

لإثبات ذلك أولا، وقبل كل شيء، إذا كان $\sigma,\tau\in G$ فإن كلا منها يحرك عددا منتهياً من العناصر في S، وبالتالي فإنه بإمكان $\sigma.\tau$ تحريك تلك العناصر من S، والتي يحركهــا على الأقل أحد العنصرين σ و τ. وعليه فإن $\sigma.\tau$ يحرك عددا منتهيا من عناصر S، وهذا يعني أن $\sigma.\tau\in G$. إن العنصر المحايد i في A(S) لا يحرك أي عنصر

من S ، ويترتب على هذا أن i يجب أن ينتمي إلى G . ولما كان قانون التجميع ، عموما ، محققا في A(S) ، فإنه كذلك محقق بالنسبة لعناصر G .

وأخـيرا إذا كان $\sigma \in G$ وكـان $x\sigma^{-1} \neq x$ ، أي ، لعـنصر ما x في S ، فإن $(x\sigma^{-1})\sigma \neq x\sigma$ ، أي $x(\sigma^{-1}o\sigma) \neq x\sigma$ ، وهذا يعني صراحة أن $x \neq x\sigma$. بعبارة أخرى ، يدل هذا على أن σ^{-1} يحرك تلك العناصر من S والتي يحركها σ وحيث إن σ يحرك عددا منتهيا من العناصر في S ، لذلك فإن هذا صحيح بالنسبة للعنصر σ^{-1} ، وبالتالي فإن σ^{-1} يجب أن ينتمي إلى G .

لقد بَيَّنَّا الآن أن G تحقق المسلمات الأربعة الأساسية التي تُعَرِّف الزمرة وذلك بالنسبة للعملية التي عيّناها . وهكذا فإن G زمرة . إن على القارىء التحقق من أن G غير منتهية وغير إبدالية .

مثال (٢-٢-٦)

لتكن G هي مجموعة المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الحقيقية بحيث إن $ad-bc \neq 0$. لنعرف على G عملية ، هي عملية ضرب المصفوفات ، أي :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{pmatrix}$$

إنه من الواضح أن عناصر هذه المصفوفة من النوع 2×2 هي أعداد حقيقية . لكي نثبت أن هذه المصفوفة تنتمي إلى G ، علينا أن نثبت أن

$$(aw+by)(cx+dz)-(ax+bz)(cw+dy) \neq 0$$

(إن هذه هي العلاقة المطلوبة بين عناصر المصفوفة لكي نجعلها تنتمي إلى G) .

بحسابات مختصرة يتضح أن :

$$(aw+by)(cx+dz)-(ax+bz)(cw+dy) = (ad-bc)(wz-xy) \neq 0$$

لأن كلا من المصفوفتين $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ و $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ تنتمي إلى G . إن قانون التجميع محقق بالنسبة لعملية ضرب المصفوفات. وبالتالي فهو محقق بالنسبة إلى G ، كما أن العنصر $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ينتمي إلى G ، لأن $1.1-0.0=1\neq 0$ ، وفضلا عن ذلك، فإن القارىء يعلم أن المصفوفة I تقوم بدور العنصر المحايد بالنسبة للعملية المعرفة على G وباستطاعته التحقق من ذلك.

وأخيرا إذا كان $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ فإنه يكون للمصفوفة

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

معنى، وذلك لأن $ad-bc \neq 0$ وبالإضافة إلى ذلك،

$$\left(\frac{d}{ad-bc}\right)\left(\frac{a}{ad-bc}\right)-\left(\frac{-b}{ad-bc}\right)\left(\frac{-c}{ad-bc}\right)=\frac{ad-bc}{(ad-bc)^2} = \frac{1}{ad-bc} \neq 0$$

وبالتالي فإن المصفوفة

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

تنتمي إلى G . كذلك فإن حسابا بسيطا يثبت أن :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

أي أن هذا العنصر هو معكوس العنصر $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. وباختصار فإن G زمرة. ومن السهل التحقق من أنها غير منتهية وغير إبدالية كذلك.

مثال (٢-٢-٧)

لتكن G هي مجموعة كل المصفوفات $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ من النوع 2×2 على مجموعة الأعداد الحقيقية بحيث إن $ad-bc=1$. ولنعرف على G عملية ضرب المصفوفات الواردة في المثال (٢-٢-٦). سنترك للقارىء التحقق من أن G زمرة، وأنها في الحقيقة غير منتهية وغير إبدالية.

نلاحظ من المثالين (٢-٢-٦) و(٢-٢-٧) أن الزمرة في المثال (٢-٢-٧) هي مجموعة جزئية من الزمرة في المثال (٢-٢-٦)، بل يمكن القول أكثر من ذلك، فبالنسبة للعملية نفسها نجد أن الزمرة الواردة في المثال (٢-٢-٧) تكون زمرة بحد ذاتها. ويمكن وصف هذا الوضع بأن نقول إن الزمرة في المثال (٢-٢-٧) **زمرة جزئية** (Subgroup) من الزمرة الواردة في المثال (٢-٢-٦). وسنتطرق فيما بعد، بشكل أوسع، إلى مفهوم الزمرة الجزئية.

مثال (٢-٢-٨)

لتكن G هي مجموعة المصفوفات $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ من النوع 2×2 حيث إن b,a عددان حقيقيان ليس كلاهما صفرا. (نستطيع أن نعبر عن هذا بقولنا إن $a^2+b^2\neq0$). باستخدام العملية نفسها المعرفة في المثالين السابقين يمكننا أن نثبت، وبسهولة، أن G زمرة إبدالية غير منتهية. هل تذكرك عملية الضرب المعرفة على G بأي شيء؟

اكتب $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ على الصيغة $aI+bJ$ حيث $J=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ، ثم احسب الضرب بدلالة هذه الحدود. ربما يثير ذلك حَدْسَك!

مثال (٢-٢-٩)

لتكن G هي مجموعة كل المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 ، حيث d,c,b,a أعداد صحيحة قياس p ، p عدد أولي، $ad-bc\neq0$. لنعرف الضرب في G كما فعلنا في المثال (٢-٢-٦)، آخذين بعين الاعتبار أن الضرب والجمع لعناصر المصفوفة هو بالنسبة لقياس العدد الأولي p . سنترك للقارىء التحقق من أن G زمرة منتهية، وغير إبدالية.

والآن نسأل كم عدد عناصر الزمرة G ؟. ربما يستنير القارىء بالحالات الخاصة $p=5, p=2$. وهنا يمكن لأيٍّ منا أن يكتب جميع عناصر G . [تنبيه! G تحتوي على 48 عنصرا عندما $p=3$] إن الجواب في الحالة العامة يتطلب معلومات لا يمكننا عرضها في هذا السياق ولعل القارىء يجرب حل هذه المسألة بنفسه.

(٢ - ٣) بعض التمهيدات الأولية

لقد تطرقنا قليلا إلى نظرية الزمر، ولكن حتى الآن لم نبرهن حقيقة واحدة حولها. لقد حان الوقت الآن لعمل ذلك. إنه، على الرغم، من أن النتائج الأولى التي سنبرهنها ليست مشوقة (بل إنها في الحقيقة مملة نوعا ما)، لكنها، مع ذلك، مفيدة جدا إذ أن تعلم حروف الهجاء لم يكن الجزء المشوق من تَعَلُّمِنا خلال طفولتنا، ولكن بعدما تعلمنا ذلك انزاحت من أمامنا العقبات وبدت الأمور أكثر تشويقا.

ونبدأ بما يلي:

تمهيدية (٢-٣-١)

إذا كانت G زمرة فإن:

(أ) العنصر المحايد في G وحيد.

(ب) لكل عنصر a في G يوجد معكوس وحيد.
(جـ) لكل عنصر a في G يكون $(a^{-1})^{-1}=a$.
(د) لكل b,a في G يكون $(a.b)^{-1}=b^{-1}.a^{-1}$.

البرهان

قد يكون من المستحسن، وقبل أن نبدأ البرهان، أن نرى ما هو الشيء الذي نريد برهانه. **في الجزء** (ا) نريد إثبات أنه إذا كان العنصران f,e في G يتمتعان بالخاصة وهي أنه إذا كان لكل a في G ، $a=a.e=e.a=a.f=f.a$ فإن $e=f$. **وفي الجزء** (ب) يكون هدفنا إثبات أنه إذا كان $x.a=a.x=e$ و $y.a=a.y=e$. لجميع العناصر y,x و a في G فإن $x=y$.

لنعتبر أولا الجزء (ا). لما كان $e.a=a$ لكل a في G ، عندئذ وبصورة خاصة، $e.f=f$. ومن ناحية أخرى، لما كان $b.f=b$ لكل b في G ، لذلك يكون لدينا $e.f=e$ ، ومن هاتين المعلومتين معا نحصل على $f=e.f=e$ ، أي أن $e=f$.

بدلا من برهان فقرة (ب)، سنبرهن نتيجة أقوى منها، والتي تكون فقرة (ا)، بطبيعة الحال، حالة خاصة منها. لنفرض أن $a.x=e$ و $a.y=e$ حيث $a\in G$. عندئذ من الواضح أن $a.x=a.y$. لنجعل هذه هي نقطة البداية بالنسبة لنا، وبمعنى آخر لنفرض أن $a.x=a.y$ حيث $a,x,y\in G$. عندئذ يوجد $b\in G$ بحيث يكون $b.a=e$ (لحد علمنا يمكن وجود عدة عناصر مثل هذا العنصر) وهكذا نجد $b.(a.x)=b.(a.y)$ واستنادا إلى قانون التجميع نجد أن:

$$x = e.x = (b.a).x = b.(a.x) = b.(a.y) = (b.a).y = e.y = y$$

لقد برهنا، في الواقع، أنه إذا كان $a.x=a.y$ في الزمرة G فإن هذا يقتضي أن يكون $x=y$.

وبالمثل يمكن برهان أنه إذا كان $x.a=y.a$ فإن $x=y$. وهذا يعني أننا يمكن أن نختزل من نفس الجانب في معادلات الزمر. ومع ذلك يجب أن ينتبه القارىء إلى أننا

لا نستطيع أن نستنتج أنه إذا كان $a.x=y.a$ فإن هذا يقتضي أن $x=y$ ، لأنه ليس لدينا أية طريقة لمعرفة ما إذا كان $a.x=x.a$. يمكن توضيح ذلك بمثال من S_3 حيث $a=\phi$ و $x=\psi$ و $y=\psi^{-1}$.

إن فقرة (جـ) تنتج من هذا وذلك بملاحظة أن $a^{-1}.(a^{-1})^{-1}=e=a^{-1}.a$ وباختزال a^{-1} من اليسار يبقى لدينا $(a^{-1})^{-1}=a$. إن هذا هو المقابل في الزمر للنتيجة المألوفة $-(-5)=5$ مثلا في زمرة الأعداد الحقيقية بالنسبة لعملية الجمع .

إن فقرة (د) هي أكثر الفقرات بساطة، لأنه

$$(a.b).(b^{-1}.a^{-1}) = a.((b.b^{-1}).a^{-1}) = a.(e.a^{-1}) = a.a^{-1} = e$$

ومن تعريف المعكوس ينتج أن $(a.b)^{-1} = b^{-1}.a^{-1}$. نورد في التمهيدية الآتية بعض النتائج المهمة التي حصلنا عليها من البرهان .

تمهيدية (٢-٣-٢)

لنفرض أن $a,b\in G$ ، عندئذ يكون للمعادلتين $a.x=b$ و $y.a=b$ حلول وحيدة في G . وبصورة خاصة فإن قانوني الاختزال (Cancellation laws) وهما إذا كان $a.u = a.w$ فإن هذا يقتضي أن يكون $u=w$ ، وإذا كان $u.a = w.a$ فإن هذا يقتضي أن يكون $u=w$ متحققان في G .

إن تفاصيل برهان هذه التمهيدية متروك للقارىء .

مسائل

١ - بيّن فيما إذا كانت الأنظمة الآتية زمرا أم لا؟ وإذا لم تكن كذلك فحدد مسلمة الزمرة التي لم تتحقق .

ا) G هي مجموعة الأعداد الصحيحة، $a.b=a-b$.

ب) G هي مجموعة الأعداد الصحيحة الموجبة و $a.b = ab$. أي أن العملية هنا هي عملية ضرب الأعداد الصحيحة .

جـ) G هي المجموعة $a_0, a_1, \ldots, a_6$ حيث $a_i.a_j=a_{i+j}$ إذا كان $i+j<7$ وإذا كان $i+j\geq 7$ فإن $a_i.a_j = a_{i+j-7}$ (على سبيل المثال، $a_4.a_5=a_{4+5-7}=a_2$ ، لأن $(4+5=9>7)$.

د) G هي مجموعة الأعداد النسبية، حيث يكون المقام عددا فرديا و $a.b=a+b$ هي عملية جمع الأعداد النسبية العادية .

٢ ـ أثبت أنه إذا كانت G إبدالية فإنه لكل $a,b\in G$ ، ولأي عدد صحيح n يكون $(a.b)^n=a^n.b^n$.

٣ ـ إذا كانت G زمرة تحقق الشرط $(a.b)^2=a^2.b^2$ لكل a ، b في G ، فأثبت أن G يجب أن تكون إبدالية .

٤*ـ إذا كانت G زمرة وكان $(a.b)^i=a^i.b^i$ من أجل ثلاث قيم صحيحة متتالية للعدد i ولكل b,a في G ، فأثبت أن G إبدالية .

٥ ـ أثبت أن الاستنتاج الوارد في المسألة ٤ لا يمكن أن يتحقق إذا افترضنا أن العلاقة $(a.b)^i=a^i.b^i$ محققة من أجل قيمتين صحيحتين متتاليتين فقط للعدد i .

٦ ـ أورد مثالا من الزمرة S_3 لعنصرين y,x بحيث يكون $(x.y)^2\neq x^2.y^2$.

٧ ـ أثبت أنه يوجد أربعة عناصر في الزمرة S_3 تحقق الشرط $x^2=e$ وثلاثة عناصر تحقق الشرط $y^3=e$.

٨ ـ إذا كانت G زمرة منتهية فأثبت أنه يوجد عدد صحيح موجب N بحيث يكون $a^N=e$ لكل a في G .

٩ ـ ا) إذا كانت G تحتوى ثلاث عناصر فأثبت أن G إبدالية .

ب) إذا كانت G تحتوي على أربعة عناصر فأثبت أن G إبدالية .

جـ) إذا كانت G تحتوي على خمسة عناصر فأثبت أن G إبدالية .

١٠ـ أثبت أنه إذا كان كل عنصر في الزمرة G هو معكوس نفسه فإن G إبدالية .

١١ـ أثبت أنه إذا كانت رتبة الزمرة G عددا زوجيا فإن G تحتوي على عنصر a ، $a\neq e$ يحقق الشرط $a^2=e$.

١٢ـ إذا كانت G مجموعة غير خالية وكانت مغلقة بالنسبة لقانون التركيب التجميعي، وحققت بالإضافة إلى ذلك مايلي :

ا) يوجد عنصر e في G بحيث يكون $a.e=a$ لكل $a\in G$.

ب) إذا كان $a\in G$ فإنه يوجد عنصر $y(a)\in G$ بحيث يكون $a.y(a)=e$.

أثبت أن G يجب أن تكون زمرة بالنسبة لهذا التركيب.

١٣- أورد مثالا تثبت فيه أن الاستنتاج الوارد في المسألة السابقة يكون غير صحيح إذا فرضنا بدلا من ذلك مايلي:

ا) يوجد عنصر $e\in G$ بحيث يكون $a.e=a$ لكل $a\in G$.

ب) إذا كان $a\in G$ عندئذ يوجد $y(a)\in G$ بحيث يكون $y(a).a=e$.

١٤- على افتراض أن المجموعة **المنتهية** G مغلقة بالنسبة للضرب التجميعي وأن قانوني الاختزال محققان في G ، أثبت أن G يجب أن تكون زمرة.

١٥- ا) باستخدام نتيجة المسألة (١٤) أثبت أن الأعداد الصحيحة غير الصفرية قياس p ، حيث p عدد أولي، تؤلف زمرة بالنسبة لعملية الضرب قياس p.

ب) طبق الجزء (ا) على الأعداد الصحيحة غير الصفرية والأولية بالنسبة إلى n وذلك بالنسبة لعملية الضرب قياس n .

١٦- أورد مثالا توضح فيه أنه إذا كان أحد قانونيْ الاختزال محققا فإنه ليس ضروريا أن تكون G زمرة.

١٧- أثبت أنه بالنسبة إلى المسألة (١٤) يوجد عدد غير نهائي من الأمثلة، التي تحقق الشرطين ولكنها ليست زمرا.

١٨- كوّن زمرة غير إبدالية رتبتها 2n ، لأي عدد n ، $n>2$ (تلميح : طبق فكرة العلاقات الواردة في S_3) .

١٩- إذا كانت S مجموعة مغلقة بالنسبة لعملية تجميعية، فأثبت أنه مهما جمّعت العناصر $a_1, a_2,...,a_r$ في أقواس مع الاحتفاظ بترتيب العناصر فإنك تحصل على العنصر نفسه من S (أي أن : $(a_1.a_2).(a_3.a_4) = a_1.(a_2.(a_3.a_4))$ استخدام الاستقراء الرياضي على n).

٢٠ - لتكن G مجموعة المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الحقيقية، بحيث إن $ad-bc\neq 0$ عدد نسبي. أثبت أن G زمرة بالنسبة لعملية ضرب المصفوفات.

٢١ - لتكن G هي مجموعة كل المصفوفات $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الحقيقية بحيث إن $ad\neq 0$ ، أثبت أن G زمرة بالنسبة لعملية ضرب المصفوفات. هل G إبدالية؟

٢٢ - لتكن G هي مجموعة المصفوفات $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ من النوع 2×2 حيث a عدد حقيقي لا يساوي الصفر. أثبت أن G زمرة إبدالية بالنسبة لعملية ضرب المصفوفات.

٢٣ - في الزمرة الواردة في المسألة (٢١) كوّن زمرة جزئية رتبتها 4 .

٢٤ - لتكن G هي مجموعة كل المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الصحيحة قياس 2 بحيث إن $ad-bc\neq o$ ، أثبت أن G زمرة رتبتها 6 ، بالنسبة لعملية ضرب المصفوفات.

٢٥ - ا) لتكن G هي زمرة كل المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الصحيحة قياس 3 بحيث إن $ad-bc\neq o$. أثبت أن $o(G)=48$. بالنسبة لعملية ضرب المصفوفات.

ب) إذا غيّرنا الشرط $ad-bc\neq o$ الوارد في الجزء (ا) إلى $ad-bc=1$ فما هي $o(G)$ ؟

٢٦* - ا) لتكن G هي زمرة كل المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الصحيحة قياس p ، حيث p عدد أولي بحيث إن $ad-bc\neq 0$ أثبت أن G تكوّن زمرة بالنسبة لعملية ضرب المصفوفات. ما هي رتبة G ؟

ب) لتكن H هي الزمرة الجزئية من الزمرة G الواردة في الجزء (ا) والمعرفة كما يلي:

$$H=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in G \mid ad-bc=1\}$$

عندئذ ما هي رتبة H ؟

(٢ - ٤) الزمر الجزئية

نود قبل استئناف دراسة الزمر أن نغيّر بعض الرموز قليلا. إن الإبقاء على استخدام الرمز « . » لعملية الضرب غير عملي، وعليه فإننا سنتخلى عنه، وعوضا عن كتابة العنصر a.b لكل a,b في G فإننا سنكتب هذا الضرب ببساطة على الصورة ab .

وعموما فإننا لن نهتم بمجموعات جزئية اختيارية من زمرة G لأن تلك المجموعات لا تعكس الحقيقة التي تنص على أن للزمرة G بنية جبرية مفروضة عليها. وأيًّا كانت المجموعات الجزئية التي نعتبرها فإنها ستكون تلك المجموعات المزودة بخواص جبرية مشتقة من خواص G . إن هذا يقودنا إلى التعريف التالي.

تعريف

يقال عن المجموعة الجزئية غير الخالية H من الزمرة G إنها ***زمرة جزئية*** *من G إذا كانت H نفسها زمرة بالنسبة للضرب المعرف على G .*

إن الملاحظة الآتية واضحة وهي أنه إذا كانت H زمرة جزئية من G و K زمرة جزئية من H فإن K زمرة جزئية من G .

قد يكون من المفيد أحيانا أن يوجد معيار لتقرير ما إذا كانت مجموعة جزئية من زمرة هي زمرة جزئية. إن هذا هو الهدف من التمهيدية الآتية.

تمهيدية (٢-٤-١)

تكون المجموعة الجزئية غير الخالية H من الزمرة G زمرة جزئية إذا وفقط إذا تحقق الشرطان:

(أ) إذا كان $a,b\in H$ فإن $ab\in H$.

(ب) إذا كان $a\in H$ فإن $a^{-1}\in H$.

البرهان

من الواضح أنه إذا كانت H زمرة جزئية من G فإن الشرطين (ا)، (ب) محققان.

ومن ناحية أخرى، لنفرض أن H مجموعة جزئية من G تحقق الشرطين (ا)، (ب). إن كل ما نحتاجه للبرهنة على أن H زمرة جزئية هو التحقق من أن $e \in H$ وأن قانون التجميع ساري المفعول بالنسبة لعناصر H . لما كان قانون التجميع محققا لعناصر الزمرة G ، لذلك فإنه أيضا محقق بالنسبة لـ H التي هي مجموعة جزئية من G. إذا كان $a \in H$ فإنه من الشرط الثاني $a^{-1} \in H$ وباستخدام الشرط الأول فإنه $e=aa^{-1} \in H$ وهذا ينهي برهان التمهيدية.

وفي الحالة الخاصة عندما تكون G منتهية فإن الوضع يصبح أبسط كثيرا، حيث إنه من الممكن الاستغناء عن الشرط الثاني.

تمهيدية (٢-٤-٢)

إذا كانت H مجموعة جزئية منتهية وغير خالية من زمرة G وكانت H مغلقة بالنسبة للضرب فإن H زمرة جزئية من G .

البرهان

على ضوء التمهيدية (٢-٤-١) سنحتاج فقط إلى إثبات أنه عندما يكون $a \in H$ فإن $a^{-1} \in H$. لنفرض أن $a \in H$ ، عندئذ $a^2=aa \in H$ و $a^3=a^2.a \in H$ و. . . . و$a^m \in H$ وذلك لأن H مغلقة وبالتالي فإن المجموعة غير المنتهية من العناصر $a, a^2, \ldots, a^m, \ldots$ لابد وأن تقع في H التي هي مجموعة جزئية منتهية من G . وبالتالي فإنه لابد وأن يوجد تكرار في هذه المجموعة من العناصر، بمعنى أنه إذا كان s,r عددين صحيحين و$r>s>0$ فإن $a^r=a^s$. ووفقا لقانون الاختزال في G نجد $a^{r-s}=e$. (وعليه فإن $e \in H$)، ولما كان $r-s-1 \geq 0$ ، لذلك فإن $a^{r-s-1} \in H$ ، كذلك فإن $a^{-1}=a^{r-s-1}$ لأن $aa^{r-s-1}=a^{r-s}=e$. وهكذا فإن $a^{-1} \in H$ وبذلك نكون قد أنهينا إثبات التمهيدية.

إن هذه التمهيدية تفيد بأنه لكي نتحقق من أن مجموعة جزئية من زمرة منتهية هي زمرة جزئية علينا أن نرى ما إذا كانت مغلقة بالنسبة لعملية الضرب أم لا .

لعلنا، نرى الآن بعض الزمر وبعض الزمر الجزئية فيها. إن الزمرة G هي دائما زمرة جزئية من نفسها، كذلك فإن المجموعة المكونة من العنصر المحايد e هي زمرة جزئية من G . إن أيا من هاتين الزمرتين ليست بذات أهمية في دراسة الزمر الجزئية، وعلى ذلك فإننا سنصفهما بالزمرتين الجزئيتين التافهتين، كما سنطلق على الزمر الجزئية الواقعة بين هاتين الزمرتين المتطرفتين اسم الزمر الجزئية غير التافهة، والتي ستكون أكثر أهمية كما سنرى الآن.

مثال (٢-٤-١)

لنفرض أن G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجميع وأن H هي المجموعة الجزئية المكونة من مضاعفات العدد 5 . على القارىء التأكد من أن H زمرة جزئية من G .

إنه لا يوجد هنا شيء غير عادي بسبب اختيار العدد 5 . وبالمثل يمكننا تعريف الزمرة الجزئية H_n بأنها تلك المجموعة الجزئية من G المكونة من مضاعفات العدد n . عندئذ تكون H_n زمرة جزئية لكل n . ماذا يمكن للمرء أن يقول عن $H_n \cap H_m$ ؟ إن من الحكمة تجربتها في حالة $H_6 \cap H_9$.

مثال (٢-٤-٢)

لتكن S أية مجموعة و A(S) زمرة التطبيقات الأحادية من S على نفسها بالنسبة لعملية تركيب التطبيقات.

ولنفرض أن $H(x_0)=\{\phi \in A(S) \mid x_0\phi=x_0\}$ حيث $x_0 \in S$ عندئذ تكون $H(x_0)$ زمرة جزئية من A(S) . إذا كان $x_1 \in S$ ، $x_1 \neq x_0$ فإننا نعرف بالمثل $H(x_1)$. ما هو $H(x_0) \cap H(x_1)$ ؟.

مثال (٢-٤-٣)

لنفرض أن G أية زمرة و $a \in G$ وأن :

$$(a) = \{a^i \mid i = 0, \pm 1, \pm 2, \ldots\}$$

عندئذ تكون (a) زمرة جزئية من G (تحقق من ذلك). إنها تدعى الزمرة الجزئية **الدورية المولدة بالعنصر** a .

إن هذا المثال يزودنا بطرق للحصول على زمر جزئية من الزمرة G . وإذا كانت G=(a) لعنصر ما a في G فإنه يطلق على G في هذه الحالة اسم **الزمرة الدورية**، إن هذه الزمرة مهمة إذ أنها تلعب دورا كبيرا في نظرية الزمر، وبخاصة في ذلك الجزء من النظرية الذي يعالج الزمر الإبدالية، وبالمناسبة، فإن الزمر الدورية هي إبدالية ولكن العكس غير صحيح .

مثال (٢-٤-٤)

لنفرض أن G زمرة، وأن W مجموعة جزئية منها، وأن (W) هي تلك المجموعة الجزئية من G والمكونة من العناصر التي يمكن كتابتها على صيغة حاصل ضرب عناصر من W مرفوعة إلى قوى صحيحة موجبة أو سالبة أو صفرا. عندئذ يطلق على (W) اسم **الزمرة الجزئية من G المولدة بـ W** وهي أصغر زمرة جزئية من G تحوى W . إن (W) ، في الواقع، هي تقاطع جميع الزمر الجزئية من G التي تحوى W (إن هذا التقاطع ليس خاليا لأن G نفسها زمرة جزئية من G التي تحتوى W).

مثال (٢-٤-٥)

لتكن G هي زمرة الأعداد الحقيقية غير الصفرية بالنسبة لعملية الضرب ولتكن H هي مجموعة الأعداد النسبية الموجبة. عندئذ تكون H زمرة جزئية من G .

مثال (٢-٤-٦)

لتكن G هي زمرة الأعداد الحقيقية بالنسبة لعملية الجمع ولتكن H هي مجموعة كل الأعداد الصحيحة. عندئذ تكون H زمرة جزئية من G .

مثال (٢-٤-٧)

لتكن G هي زمرة المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2×2 على مجموعة الأعداد الحقيقية حيث $ad-bc\neq 0$ بالنسبة لعملية ضرب المصفوفات ولتكن $H=\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\in G|ad\neq 0\}$ ، عندئذ تكون H زمرة جزئية من G ويمكن التحقق من ذلك بسهولة .

مثال (٢-٤-٨)

لتكن H هي الزمرة المعرفة في المثال (٢-٤-٧) ولتكن $K=\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$ ، عندئذ تكون K زمرة جزئية من H .

مثال (٢-٤-٩)

لتكن G هي زمرة كل الأعداد المركبة غير الصفرية من الصيغة $a+bi$ (حيث b,a أعداد حقيقية ليست كلها أصفارا) وذلك بالنسبة لعملية الضرب ولتكن $H=\{a+bi|a^2+b^2=1\}$ ، أثبت أن H زمرة جزئية من G .

تعريف

لتكن G زمرة و H زمرة جزئية من G . ولنفرض أن $a,b\in G$ ، نقول إن a يطابق b قياس H ونكتب $a\equiv b \bmod H$ إذا كان $ab^{-1}\in H$.

تمهيدية (٢-٤-٣)

إن العلاقة $a\equiv b \bmod H$ هي علاقة تكافؤ.

البرهان

بالرجوع إلى الفصل الأول نجد أنه لكي نبرهن على التمهيدية (٢-٤-٣) يجب علينا تحقيق الشروط الثلاثة الآتية لكل $a,b,c\in G$:

١) $a\equiv a \bmod H$

٢) إذا كان $a \equiv b \bmod H$ فإن $b \equiv a \bmod H$

٣) إذا كان $a \equiv b \bmod H$ و $b \equiv c \bmod H$ فإن $a \equiv c \bmod H$

دعنا الآن نتحقق من كل شرط من هذه الشروط على انفراد.

١) لكي نثبت أن $a \equiv a \bmod H$ ، يجب علينا أن نبرهن، وذلك باستخدام تعريف التطابق قياس H أن $aa^{-1} \in H$. لما كانت H زمرة جزئية من G و $e \in H$ ، ولما كان $aa^{-1}=e$ ، لذلك نجد أن $aa^{-1} \in H$. وهذا هو المطلوب إثباته.

٢) لنفرض أن $a \equiv b \bmod H$ ، أي لنفرض أن $ab^{-1} \in H$ ونريد أن نثبت أن $b \equiv a \bmod H$ أو بعبارة أخرى، أن $ba^{-1} \in H$. لما كان $ab^{-1} \in H$ ، ولما كانت H زمرة جزئية، لذلك فإن $(ab^{-1})^{-1} \in H$. ولكن من التمهيدية (٢-٣-١) $(a\, b^{-1})^{-1}=(b^{-1})^{-1}a^{-1}=b\, a^{-1}$ وبالتالي $ba^{-1} \in H$ أي أن $b \equiv a \bmod H$.

٣) بقي علينا برهان أنه إذا كان $a \equiv b \bmod H$ و$b \equiv c \bmod H$ فإن $a \equiv c \bmod H$.
من التطابق الأول والثاني نحصل على $ab^{-1} \in H$ و $bc^{-1} \in H$ على الترتيب.
وحيث إن H زمرة جزئية من G ، لذلك نجد أن:
$(ab^{-1})(bc^{-1}) \in H$ ومع ذلك، $a\, c^{-1}= aec^{-1}=a(b^{-1}b)c^{-1}=(a\, b^{-1})(bc^{-1})$ وبالتالي نجد أن $ac^{-1} \in H$ ، أي أن $a \equiv c \bmod H$

إن هذا يؤكد أن علاقة التطابق قياس H هي علاقة تكافؤ وعليه فإننا سنوظف جميع النتائج المتعلقة بعلاقات التكافؤ والتي تعرفنا عليها في الباب الأول في دراسة هذه العلاقة الخاصة.

بقيت كلمة قصيرة حول الرمز الذي استخدمناه. إذا كان G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع وكانت $H=H_n$ هي الزمرة الجزئية من G المكونة من مضاعفات العدد n ، فإن العلاقة $a \equiv b \bmod H_n$ أي $ab^{-1} \in H_n$ تعني بالنسبة لعملية الجمع هنا أن $a-b$ هو مضاعف للعدد n وهذا هو التطابق قياس n العادي والمعرف في نظرية الأعداد.

وبعبارة أخرى، إن العلاقة التي عرفناها باستخدام زمرة جزئية من زمرة ما، ما هي إلا تعميم لعلاقة مألوفة في زمرة أَلِفْنَاها من قبل.

تعريف

إذا كانت H زمرة جزئية من G و $a \in G$ فإن المجموعة $Ha=\{ha/h \in H\}$ تسمى ***بالمجموعة المشاركة اليمنى لـ H في G*** .

تمهيدية (٢-٤-٤)

لكل $a \in G$ يكون

$$Ha= \{x \in G/a \equiv x \bmod H\}$$

البرهان

لنفرض أن $[a]= \{x \in G|a \equiv x \bmod H\}$ ، ونثبت أولا أن $Ha \subset [a]$.

لذلك، إذا كان $h \in H$ فإن $a(ha)^{-1}=a(a^{-1}h^{-1}) = h^{-1} \in H$ لأن H زمرة جزئية من G. وهذا يقتضي، استنادا إلى تعريف التطابق قياس H ، أن $ha \in [a]$ لكل $h \in H$ ، وعليه فإن $Ha \subset [a]$.

لنفرض، الآن، أن $x \in [a]$ ، عندئذ يكون $ax^{-1} \in H$ وبالتالي يكون $(ax^{-1})^{-1}=xa^{-1} \in H$ وهذا يعني أن $xa^{-1}=h$ حيث $h \in H$. بضرب الطرفين من اليمين بالعنصر a نجد أن $x=ha$ ، أي أن، $x \in Ha$ ويترتب على ذلك أن $[a] \subset Ha$. وهكذا نكون قد برهنا على الاحتوائين $[a] \subset Ha$ و $Ha \subset [a]$ ، ومن ذلك نستنتج أن $[a]=Ha$ مما ينهي البرهان.

ووفقا لاصطلاح الفصل الأول فإن $[a]$ ، ومثله Ha هو فصل تكافؤ العنصر a في G . واستنادا إلى مبرهنة (١-١-١) فإن فصول التكافؤ هذه تقتضي تحليل G إلى

مجمـوعـات جزئية منفصلة. وعليه فإن أي مجمـوعتين مشاركتين Ha و Hb في G إما **متطابقتان أو منفصلتان**.

إننـا ندّعي الآن وجـود تقـابـل بين أي مجمـوعتين مشاركتين يمنيين Ha وHb لـH في G ، بعبـارة أخـرى، نقـابـل العنصر $ha \in Ha$ لأي عنصر $h \in H$ ، بالعنصر $hb \in Hb$. إنه من الواضح أن هذا التطبيق غامر. ونثبت الآن أنه أحادي كما يلي:

إذا كان $h_1b=h_2b$ حيث $h_1, h_2 \in H$ فإنـه وفقـا لقانون الاختزال في G نجد أن $h_1=h_2$ ، أي أن $h_1a=h_2a$. إن هذا يثبت التمهيدية الآتية.

تمهيدية (٢-٤-٥)

يوجد تقابل بين أي مجموعتين مشاركتين يمينيتين لـ H في G .

عندما تكون H زمرة منتهية فإن للتمهيدية **(٢-٤-٥)** فائدة كبرى لأنها تنص على أن أي مجموعتين مشاركتين يمنيين لـH في G تحتويان على العدد نفسه من العناصر، ولكن كم عنصرا يمكن أن تحتويه المجموعة المشاركة اليمنى لـH في G ؟

حسنا، لاحظ أن H=He هي نفسها مجموعة مشاركة يمنى لـH . وبالتالي فإن أية مجموعة مشاركة يمنى لـH في G تحتوي على عناصر عددها o(H) .

لنفــرض أن G زمــرة منتهية وأن k هو عدد المجمـو عات المشـاركـة اليمنى المختلفـة لـH في G . من التمهيديتين **(٢-٤-٤)**، **(٢-٤-٥)** نجد أن أي مجموعتين مشاركتين يمنيين مختلفتين لـH في G منفصلتان كما أن كلا منهما تحتوي على عناصر عددهــا o(H) . ولـما كان أي عنصر $a \in G$ ينتمي إلى المجمـوعـة المشـاركـة اليمنى الـوحيدة Ha ، لذلك، فإن المجموعات المشاركة اليمنى تغطي G . وهكذا، إذا كان k يمثـل عدد المجمـوعـات المشـاركة اليمنى لـH في G ، فإنه يجب أن يكون لدينا

$ko(H)=o(G)$ ، وبهـذا نكـون قد أثبتنا المبرهنة الشهيرة الآتية المنسوبة إلى لاجرانج (Lagrange) .

مبرهنة (٢-٤-١)

إذا كانت G زمرة منتهية وكانت H زمرة جزئية منها فإن $o(H)$ قاسم لـ $o(G)$.

تعريف

*إذا كانت H زمرة جزئية من G فإن **دليل** $H(index)$ في G هو عدد المجموعات المشاركة اليمنى المختلفة لـH في G .*

سنـرمز لهذا العدد بالرمز $i_G(H)$. وعندما تكون G منتهية فإن $i_G(H)=\frac{o(G)}{o(H)}$ ، كما هو واضح من إثبات مبرهنة لاجرانج . إن من الممكن تماما وجود زمرة غير منتهية تحتوي على زمرة جزئية فعلية H بحيث يكون دليل H في G منتهيا .

قد يكون من الصعب هنا أن يدرك الطالب الأهمية البالغة لهذه النتيجة ولكن كلما تغلغـل الإنسـان أكثـر في المـوضوع فإنه سيجد نفسه مدركا أكثر فأكثر لمميزاته الأساسية . ونظرا لما لهذه المبرهنة من أهمية ، لذلك فإنها تستحق تدقيقا عن كثب وكذلك تحليلا أكثر . وفيما يلي ، نورد طريقة مختلفة للوقوف على برهانها . في الحقيقة ، إن الطريقة التي سنلخصها فيما بعد ليست مختلفة عن تلك التي أوردناها آنفا . إن تقديم التطابق قياس H يسهل كتابة العناصر المستخدمة فيما بعد ، كما أنه يتجنب الحاجة إلى التأكد من أن العناصر الجديدة والمقدمة في كل مرحلة لم تظهر من قبل .

لذلك ، نفرض مرة أخرى أن G زمرة منتهية وأن H زمرة جزئية منها عناصرها هي $h_1, h_2, \ldots, h_r$ ، حيث $r=o(H)$.

إذا كانت $H=G$ فإنه لا يوجد شيء يستدعي البرهان . لذلك نفرض أن $H\neq G$ عندئذ يوجد عنصر $a\in G$ بحيث يكون $a\notin H$.

لنكتب جميع العناصر التي حصلنا عليها في صفين كما يلي:

$$h_1, h_2, \ldots\ldots., h_r$$

$$h_1a, h_2a, \ldots\ldots., h_ra$$

إننا ندعي أن جميع العناصر في الصف الثاني مختلفة عن بعضها البعض كما أنها مختلفة عن العناصر في الصف الأول، ذلك أنه لو كان أي عنصرين من الصف الثاني متساويين، أي $h_ia=h_ja$ ، $i \neq j$ فإنه من قانون الاختزال نجد أن $h_i=h_j$ وهذا تناقض. ولو كان عنصر من الصف الأول مساويا لعنصر من الصف الثاني، أي $h_ia=h_j$ فإن هذا يقتضي أن $a=h_i^{-1} h_j \in H$ لأن H زمرة جزئية من G وهذا يناقض كون $a \notin H$.

إلى هنا، نكون قد حصلنا على عناصر عددها $2o(H)$. فإذا كان هذا العدد هو عدد عناصر G ، فإننا نكون قد انتهينا من البرهان. وإن لم يكن الأمر كذلك فإنه يوجد عنصر $b \in G$ لا ينتمي إلى كل من الصفين المذكورين آنفا. لنعتبر القائمة الجديدة.

$$h_1, h_2, \ldots\ldots., h_r$$

$$h_1a, h_2a, \ldots\ldots., h_ra$$

$$h_1b, h_2b, \ldots\ldots., h_rb$$

إن بإمكاننا كما فعلنا سابقا أن نثبت أنه لا يوجد عنصران متساويان في الصف الثالث، كما لا يوجد عنصر من الصف الثالث مساوٍ لعنصر من الصف الثاني أو الأول. وهكـذا نكون قد كوّنا قائمة من العناصر التي عددها $3\,o(H)$. بالاستمرار في هذه الـطريقـة نجـد أن كل عنصر جديد يستحـدث ينتج، في الحقيقة، عناصر جديدة عددها $o(H)$. ونظرا لكون G منتهية فإننا يجب أن نأتي على جميع عناصر G . ولكن إذا انتهينا باستخدام صفوف عددها k لكي تشمل هذه الصفوف جميع عناصر G ، فإن بوسعنا أن نكتب قائمة بعناصر مختلفة عددها $k\,o(H)$ ، وبناءً عليه فإن $k\,o(H)=o(G)$.

إن من الضروري أن نعلم أن عكس مبرهنة لاجرانج ليس صحيحا، بمعنى أنه ليس من الضروري إذا كان $m|o(G)$ ، فإن G تحتوي على زمرة جزئية رتبتها m .

فعلى سبيل المثال، توجد زمرة رتبتها 12 ولكنها لا تحتوي على زمرة جزئية رتبتها 6 . ويمكن للقارىء أن يحاول إيجاد مثال آخر لهذه الظاهرة؛ والزمرة التي يمكن أن ينظر إليها هي في الزمرة S_4 ، زمرة التناظر من الدرجة الرابعة التي تحتوي على زمرة جزئية رتبتها 12 والتي تحقق ما نريد.

إن مبرهنة لاجرانج تشتمل على نتائج في غاية الأهمية، ولكن قبل أن نعرض هذه النتائج نعطي التعريف الآتي:

تعريف

إذا كانت G زمرة و $a \in G$ فإن رتبة (order) (أو دور (period)) a هي أقل عدد صحيح موجب n بحيث إن $a^n=e$.

وإذا لم يوجد مثل هذا العدد الصحيح فإننا نقول إن رتبة a غير منتهية. وسنرمز لرتبة العنصر a بالرمز o(a) . لنعيد إلى الذاكرة رمزا استخدمناه سابقا هو أنه إذا كان لدينا العددان v,u فإن $u|v$ يعني أن u قاسم لـ v .

نتيجة (١)

إذا كانت G زمرة منتهية و $a \in G$ فإن $o(a)|o(G)$.

البرهان

إنه يبدو طبيعيا، حيث مبرهنة لاجرانج في متناول أيدينا، أن نبرهن على صحة النتيجة عن طريق تكوين زمرة جزئية من G رتبتها o(a). إن العنصر a نفسه يزودنا بهذه الزمرة الجزئية وذلك باعتبار الزمرة الجزئية الدورية (a) من G المولدة بالعنصر a ؛ إن (a) تتكون من العناصر $e,a,a^2,\ldots$. إن السؤال الذي يطرح نفسه هو كم عدد العناصر في (a) ؟

إننا نزعم أن هذا العدد هو o(a) . من الواضح أن هذه الزمرة الجزئية تحتوي على عناصر عددها o(a) على الأكثر، ذلك لأن $a^{o(a)}=e$ ، وإذا كانت تحتوي على عناصر

عددها أقل من $o(a)$ فإن هذا يعني أن $a^i=a^j$ ، حيث $0 \le i<j<o(a)$ ، وعندئذ $a^{j-i}=e$ ، $0<j-i<o(a)$ ، ولكن هذا يناقض تعريف $o(a)$. وبناءً عليه فإن الزمرة الجزئية المولدة بالعنصر a تحتوي على عناصر عددها $o(a)$ ، واستنادا إلى مبرهنة لاجرانج نجد أن $o(a)|o(G)$.

نتيجة (٢)

إذا كانت G زمرة منتهية و $a \in G$ فإن $a^{o(G)}=e$.

البرهان

وفقا لنتيجة (١)، $o(a)|o(G)$ ؛ لذلك يكون $o(G)=mo(a)$ وبناءً عليه

$$a^{o(G)} = a^{mo(a)} = (a^{o(a)})^m = e^m = e$$

حالة خاصة من هذه النتيجة ذات أهمية عظمى في نظرية الأعداد تتعلق بما يسمى **بدالة أويلر** ϕ(Euler) والتي تعرف لجميع الأعداد الصحيحة الموجبة n كما يلي:

$\phi(1) = 1$ ؛ وإذا كان $n>1$ فإن $\phi(n)$ هو عدد الأعداد الصحيحة الموجبة التي هي أقل من n وأولية بالنسبة إلى n . وهكذا، وعلى سبيل المثال، $\phi(8)=4$ ، لأن 1,3,5,7 هي فقط الأعداد التي أقل من 8 وأولية بالنسبة إليه.

في المسألة **١٥**(ب) التي في نهاية البند **(٢-٣)** مطلوب من القارىء أن يبرهن على أن الأعداد التي أقل من n وأولية بالنسبة إليه تؤلف زمرة وذلك بالنسبة لعملية الضرب على مجموعة الأعداد الصحيحة قياس n . إن رتبة هذه الزمرة هي $\phi(n)$. وبتطبيق النتيجة (٢) على هذه الزمرة نحصل على:

نتيجة (٣) (أويلر Euler)

إذا كان n عددا صحيحا موجبا وكان a أوليا بالنسبة إلى n فإن $a^{\phi(n)} \equiv 1 \bmod n$.

لكي نطبق نتيجة (٢)، يجب استبدال a بباقي قسمته على n فإذا كانت n عددا أوليا وليكن p ، فإن $\phi(p)=p-1$. وإذا كان a عددا صحيحا أوليا بالنسبة إلى p فإنه وفقا لنتيجة (٣) $a^{p-1}\equiv 1 \mod p$ ، ومن ثم فإن $a^p\equiv a \mod p$.

ومن ناحية أخرى، إذا كان a ليس أوليا بالنسبة إلى p ، وحيث إن p عدد أولي فإنه يجب أن يكون لدينا $p|a$ ، وبناءً عليه، فإن $a\equiv 0 \mod p$ ، وبالتالي $0\equiv a^p\equiv a \mod p$ وبهذا نكون قد برهنا النتيجة التالية.

نتيجة (٤) (فيرما Fermat)

إذا كان p عددا أوليا، وكان a هو أي عدد صحيح فإن $a^p\equiv a \mod p$.

نتيجة (٥)

إذا كانت G زمرة منتهية رتبتها عدد أولي p فإن G زمرة دورية .

البرهان

إننا ندَّعي أن G لا تحتوي على زمرة جزئية غير تافهة H ؛ لأنه إذا وجدت مثل هذه الزمرة فإن $o(H)$ يجب أن يقسم $o(G)$ التي تساوي p وعليه فإنه يوجد احتمالان هما $o(H)=1$ أو $o(H)=p$ إن الاحتمال الأول يقتضي أن $H=(e)$ ، بينما الثاني يقتضي أن $H=G$.

لنفرض الآن أن $a\in G$ حيث $a\neq e$ ، وأن $H=(a)$. عندئذ تكون H زمرة جزئية من G ، $H\neq(e)$ ، لأن $a\in H$ ، $a\neq e$. وهكذا فإن $H=G$ مما يعني أن G دورية وأن كل عنصر من G هو إحدى قوى a .

إن لهذا البند أهمية كبرى لما سيرد لاحقا، وليس ذلك راجعا إلى نتائجه بل لأن روح البراهين المقدمة هنا متأصلة فيها نظرية الزمر. ومن المتوقع أن يقابل القارىء أمورا

أخرى على هذا النمط. ومن الأفضل أن يستوعب القارىء المادة الواردة هنا بصورة أعمق قبل أن يواجه نظريات لا يستطيع استيعابها وذلك قبل فوات الأوان.

(٢ـ٥) أحد مبادىء العدّ

لقد عرّفنا سابقا، أنه إذا كانت H زمرة جزئية من G و $a \in G$ فإن Ha هي مجموعة كل العناصر في G من الصيغة ha حيث $h \in H$. دعنا الآن نعمم هذه الفكرة فإذا كانت H و K زمرتين جزئيتين من G فإن:

$$HK = \{x \in G | x = hk, h \in H, k \in K\}$$

الآن نلقي نظرة على هذا المثال. لنفرض أن $G=S_3$ وأن $H=\{e,\phi\}$ و $K=\{e,\phi\psi\}$.

ماذا يمكن أن نقول عن HK ؟

استنادا إلى تعريف HK ، نرى أن HK تتكون من العناصر $e,\phi,\phi\psi,\phi^2\psi=\psi$ وحيث إن HK تتكون من أربعة عناصر، وحيث إن العدد 4 ليس قاسما للعدد 6 الذي هو رتبة S_3 ، لذلك فإنه وفقا لمبرهنة لاجرانج نجد أن HK ليست زمرة جزئية من S_3 . (بالطبع يمكننا التحقق من ذلك مباشرة ولكن هذا لا يمنع من التذكير بمبرهنة لاجرانج) إن بإمكاننا أن نبحث عن سبب عدم كون HK زمرة جزئية.

لاحظ أن:

$$KH = \{e, \phi, \phi\psi, \phi\psi\phi = \psi^{-1}\} \neq HK$$

وهذا هو بالفعل سبب عدم كون HK زمرة جزئية، كما سنرى ذلك في التمهيدية الآتية.

تمهيدية (٢ـ٥ـ١)

إن HK زمرة جزئية من G إذا وفقط إذا كان KH=HK .

البرهان

لنفرض، أولا، أن HK=KH ، أي أنه إذا كان $h \in H$ و $k \in K$ ، فإن $hk = k_1h_1$ حيث $k_1 \in K, h_1 \in H$ (ليس ضروريا هنا أن يكون $k_1=k$ أو $h_1=h$).

لبرهان أن HK زمرة جزئية يجب علينا التحقق من أنها مغلقة وأنه يوجد لكل عنصر في HK معكوس في HK . لنثبت أولا خاصة **الإغلاق**. لنفرض أن $x=hk\in HK$ وأن $y=h'k'\in HK$. فيكون $xy=hkh'k'$ ، ولكن $kh'\in KH=HK$ وبالتالي $kh'=h_2k_2$ ، حيث $h_2\in H$ و $k_2\in K$ ، وبناءً عليه فإن،

$$xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK$$

ومن ثم فإن HK مغلقة. كذلك فإن $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH=HK$ ، أي أن $x^{-1}\in HK$ ومن ثم فإن HK زمرة جزئية من G .

ومن ناحية أخرى، إذا كانت HK زمرة جزئية من G فإنه لأي $h\in H$ و $k\in K$ يكون $h^{-1}k^{-1}\in HK$ ، وهكذا فإن $kh=(h^{-1}k^{-1})^{-1}\in HK$ ، أي أن $KH\subset HK$.

الآن، إذا كان x أي عنصر من HK فإن $x^{-1}=hk\in HK$ ، وعليه فإن

$$x=(x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1}\in KH$$

أي أن $HK\subset KH$. وبهذا نكون قد أثبتنا أن $HK=KH$.

حالة خاصة من هذه التمهيدية هي عندما تكون G إبدالية، في هذه الحالة يكون $HK=KH$ ونتيجة لهذا يكون لدينا.

نتيجة

إذا كانت *H, K زمرتين جزئيتين من الزمرة الإبدالية G فإن HK زمرة جزئية من G* .

لقد رأينا أنه إذا كانت K,H زمرتين جزئيتين من G فإنه ليس ضروريا أن تكون HK زمرة جزئية من G . إن السؤال الذي يطرح نفسه بعد هو: ما هو عدد العناصر المختلفة الموجودة في المجموعة الجزئية HK ؟ إذا رمزنا لهذا العدد بالرمز $o(HK)$ فإنه تكون لدينا المبرهنة الآتية.

مبرهنة (٢-٥-١)

إذا كانت K,H زمرتين جزئيتين منتهيتين من الزمرة G وكانت $o(H)$ و $o(K)$ هما رتبتا K,H على الترتيب فإن

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$$

البرهان

على الرغم من أنه لا توجد حاجة لكي نركز انتباهنا على الحالة الخاصة التي يكون عندها $H \cap K = (e)$. ولكنه بالنظر لمثل هذه الحالة يمكننا استنتاج حقائق عن الحالة العامة. هنا يجب أن نبحث كيفية إثبات أن $o(HK) = o(H)\, o(K)$. ونسأل أنفسنا ما الذي يمنع من حدوث هذه المساواة؟.

من الواضح أن الجواب هنا هو أنه بكتابة جميع العناصر hk حيث $h \in H$ و $k \in K$ فإنه يوجد بعض التكرار، بمعنى أن بعض العناصر في القائمة يمكن أن تظهر مرتين على الأقل.

بعبارة أخرى، يكون $hk = h_1k_1$ حيث $h_1 \neq h$ ، $h, h_1 \in H$ ولكن عندئذ يكون $h_1^{-1}h = k_1k^{-1}$ ولما كان $h_1 \in H$ لذا فإن $h_1^{-1} \in H$ أيضا ومن ثم فإن $h_1^{-1}h \in H$ وبالمثل $k_1k^{-1} \in K$. وبما أن $h_1^{-1}h = k_1k^{-1}$ لذلك نجد $h_1^{-1}h \in H \cap K = (e)$ وبناءً عليه فإن $h_1^{-1}h = e$ وهذا يقضي أن $h_1 = h$ مما يناقض كون $h_1 \neq h$. وهكذا نكون قد برهنا على أنه لا يمكن وجود أي تكرار، أي أن $o(HK)$ تساوي بالفعل $o(H)\, o(K)$.

الآن، بالاستعانة بما أثبتناه في الفقرة أعلاه، يمكننا برهان الحالة العامة وكما رأينا آنفا، يجب أن نطرح السؤال: كم مرة يمكن للعنصر hk أن يظهر على هيئة حاصل ضرب في قائمة عناصر HK ؟ إننا ندَّعي أنه يجب أن يظهر $o(H \cap K)$ من المرات!. لكي ترى ذلك، نلاحظ أولا أنه إذا كان $h_1 \in H \cap K$ فإن

$$hk = h\,h_1\,(h_1^{-1}k) \qquad (١)$$

حيث $hh_1 \in H$ ، لأن $h \in H$ ، $h_1 \in H \cap K \subset H$ وكذلك $h_1^{-1}k \in K$ لأن $h_1^{-1} \in H \cap K \subset K$ و $k \in K$. وهكذا فإن العنصر hk مكرر في حاصل الضرب على الأقل $o(H \cap K)$ مرة. ومع ذلك إذا كان $hk = h'k'$ فإن $h^{-1}h' = k(k')^{-1} = u$ و $u \in H \cap K$. وبناءً عليه فإن $h' = hu$ و $k' = u^{-1}h$ ، مما يعني أن جميع التكرارات قد أخذت في الحسبان كما في (١). وبالتالي فإن العنصر hk يظهر في قائمة عناصر HK بالضبط $o(H \cap K)$ مرة. وهكذا فإن عدد العناصر المختلفة في HK هو العدد الكلي في قائمة HK ، أي $o(H)o(K)$ ، مقسوما على عدد تكرار عنصر ما، أي $o(H \cap K)$ مما يثبت المبرهنة.

لنفرض الآن أن K,H زمرتان جزئيتان من الزمرة المنتهية G وأن $o(H) > \sqrt{o(G)}$ و $o(K) > \sqrt{o(G)}$. عندئذ بما أن $HK \subset G$ فإن $o(HK) \leq o(G)$ ، ومع ذلك،

$$o(G) \geq o(HK) = \frac{o(H)o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)}$$

وهكذا فإن $o(H \cap K) > 1$ وبناءً عليه فإن $H \cap K \neq (e)$. بهذا نكون قد أثبتنا النتيجة الآتية.

نتيجة

إذا كانت K,H زمرتين جزئيتين من G وكانت $o(H) > \sqrt{o(G)}$ و $o(K) > \sqrt{o(G)}$ فإن $H \cap K \neq (e)$.

لنطبق هذه النتيجة على الحالة الخاصة الآتية. لنفرض أن G زمرة منتهية رتبتها pq حيث p و q عددان أوليان و $p > q$. إننا ندّعي أن G يمكن أن تحتوي على زمرة جزئية واحدة على الأكثر رتبتها p .

لبرهان ذلك، لنفرض أن H , K زمرتان جزئيتان رتبة كل منهما p . من النتيجة السابقة $H \cap K \neq (e)$. ونظرا لكون $H \cap K$ زمرة جزئية من H ، كذلك لما كانت رتبة H عددا أوليا، ولما كانت H لا تحتوي على زمر جزئية غير تافهة، فإننا نستنتج أن $H \cap K = H$ ، وبناءً عليه فإن $H \subset H \cap K \subset K$ ، وبالمثل $K \subset H$ ، ومن ثم فإن $H = K$ مثبتين بذلك أنه يوجد على الأكثر زمرة جزئية واحدة رتبتها تساوي p . وسنرى فيما بعد أنه يوجد على الأقل زمرة جزئية واحدة رتبتها تساوي p ، وهذا مع ما سبق يفيدنا أنه يوجد تماما زمرة جزئية واحدة في G رتبتها تساوي p . وبهذا نكون قادرين تماما على تعيين بُنية الزمرة G .

مسائل

١ - إذا كانت H , K زمرتين جزئيتين من G فأثبت أن $H \cap K$ زمرة جزئية من G (هل بإمكانك أن ترى أن البرهان نفسه يثبت أن تقاطع أي عدد سواء كان منتهيا أو غير منته من الزمر الجزئية في G هو أيضا زمرة جزئية في G ؟).

٢ - لتكن G زمرة بحيث يكون تقاطع جميع زمرها الجزئية التي لا تساوي (e) هو زمرة جزئية لا تساوي (e) . أثبت أن رتبة كل عنصر من G يجب أن تكون منتهية.

٣ - إذا كانت G لا تحتوي على زمر جزئية غير تافهة، فأثبت أن G يجب أن تكون منتهية ورتبتها عدد أولي.

٤ - ا) إذا كانت H زمرة جزئية من G وكان $a \in G$ و $aHa^{-1} = \{aha^{-1} | h \in H\}$ فأثبت أن aHa^{-1} زمرة جزئية من G .

ب) إذا كانت H منتهية فما هي رتبة aHa^{-1} ؟

٥ - لنعرف المجموعة المشاركة اليسرى للزمرة الجزئية H من G والتي نرمز لها بالرمز aH بأنها مجموعة كل العناصر من الصيغة ah حيث $h \in H$ أثبت أنه يوجد تقابل أحادي بين المجموعات المشاركة اليسرى واليمنى لـH في G .

٦ - اكتب جميع المجموعات المشاركة اليمنى لـ H في G حيث:

ا) $G=(a)$ هي الزمرة الدورية التي رتبتها تساوي 10 و $H=(a^3)$ هي الزمرة الجزئية من G المولدة بالعنصر a^3 .

ب) G هي الـزمرة نفسها الواردة في الفقرة (ا)، وH هي الزمرة الجزئية المولدة بالعنصر a^5 .

جـ) $G=A(S)$ حيث $S=\{x_1, x_2, x_3\}$ و $H=\{\sigma\in G|x_1\sigma=x_1\}$.

٧ ـ اكتب جميع المجموعات المشاركة اليسرى لـ H في G حيث G وH كما في المسألة (٦) .

٨ ـ في المسألة (٦) هل كل مجموعة مشاركة يمنى هي مجموعة مشاركة يسرى لـ H في G .

٩ ـ لنفـرض أن H زمـرة جزئية من G بحيث إنـه عنـدمـا تكـون $Ha\neq Hb$ فإن $aH\neq bH$. أثبت أن $gHg^{-1}\subset H$ لكل $g\in G$.

١٠ـ لتكن G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع وH_nهي الزمرة الجزئية من G المكـونـة من مضـاعفات العدد n . عين دليل H_n في G ثم اكتب جميع المجموعات المشاركة اليمنى لـH_n في G .

١١ـ في المسألة (١٠) ما هو $H_n\cap H_m$ ؟

١٢ـ إذا كانت G زمرة و K,H زمرتين جزئيتين من G بحيث يكون دليل كل منهما في G عددا منتهيا . أثبت أن دليل $H\cap K$ في G هو عدد مُنتهٍ أيضا . هل تستطيع إيجاد حد أعلى لدليل $H\cap K$ في G ؟

١٣ـ لنفرض أن $a\in G$ ولنعرف المجموعة $N(a)=\{x\in G|xa=ax\}$. أثبت أن $N(a)$ زمرة جزئية من G . يطلق على $N(a)$ **منظم أو ممركز** (Normalizer or Centralizer) العنصر a في G .

١٤ـ إذا كانت H زمرة جزئية من G ، فإننا نعرف **ممركز** H الذي نرمز له بالرمز $C(H)$ بأنه مجموعة العناصر $x\in G$ بحيث إن $xh=hx$ لكل $h\in H$. برهن على أن $C(H)$ زمرة جزئية من G .

١٥ـ يعـرف **مركز** (Centre) الزمرة G ويرمز له بالرمز Z بأنه مجموعة العناصر $z\in G$ بحيث يكون $zx=xz$ لكل $x\in G$. أثبت أن Z زمرة جزئية من G . هل تستطيع التحقق من أن $Z=C(T)$ لزمرة جزئية Tمن G ؟

١٦- إذا كانت H زمـرة جزئية من G و $N(H) = \{a\in G|aHa^{-1}=H\}$ (انظر مسألة ٤ فقرة ا) أثبت أن :

ا) $N(H)$ زمرة جزئية من G .

ب) $N(H)\supset H$

١٧- أورد مثالا لزمرة جزئية H من زمرة G بحيث يكون $N(H)\neq C(H)$. هل توجد أية علاقة احتواء بين $N(H)$ و $C(H)$ ؟

١٨- لتكن $N=\bigcap_{x\in G} xHx^{-1}$ حيث H زمـرة جزئية من G . أثبت أن N زمرة جزئية من G بحيث إن $aNa^{-1}=N$ لكل a في G .

١٩*- إذا كان دليل الزمرة الجزئية H في G منتهيا ، فأثبت أنه يوجد عدد منته من الزمر الجزئية المختلفة في G من الصيغة aHa^{-1} .

٢٠*- إذا كان دليل الزمرة الجزئية H من G منتهيا . فأثبت أنه يوجد زمرة جزئية N من G و N محتواة في H كما أن دليل N في G منته بحيث إن $aNa^{-1}=N$ لكل $a\in G$.
هل تستطيع إعطاء حد أعلى لدليل N في G ؟

٢١- ليكن τ_{ab} هو التطبيق من مجموعة الأعداد الحقيقية إلى نفسها المعرف بالقاعدة $\tau_{ab}:x\to ax+b$ ، حيث b,a عددان حقيقيان ولتكن $G=\{\tau_{ab}|a\neq 0\}$. أثبت أن G زمرة بالنسبة لعملية تركيب التطبيقات . أوجد صيغة للتطبيق $\tau_{ab}\tau_{cd}$.

٢٢- في المسـألة (٢١)، لتكن H هي المجموعة الجزئية من G المكونة من العناصر τ_{ab} بحيث يكون a عددا نسبيا . أثبت أن H زمرة جزئية من G . اكتب قائمة جميع المجموعات المشاركة اليمنى لـH في G وقائمة جميع المجموعات المشاركة اليسرى لـH في G . ومن ذلك أثبت أن أية مجموعة مشاركة يسرى لـH في G هي مجموعة مشاركة يمنى .

٢٣- لتكن $N=\{\tau_{1b}\in G\}$ ، حيث G هي الزمرة الواردة في المسألة (٢١) . أثبت ما يلي :

ا) N زمرة جزئية من G .

ب) إذا كان $a\in G$ و $n\in N$ فإن $ana^{-1}\in N$.

٢٤*- لتكن G هي الـزمـرة المنتهية التي رتبتهـا لا تقبل القسمة على 3 ولنفرض أن $(ab)^3=a^3b^3$ لكل b,a في G . أثبت أن G يجب أن تكون إبدالية .

٢٥*- لتكن G زمرة إبدالية ولنفرض أن G تحتوي على عنصرين رتبتاهما n,m على الترتيب. أثبت أن G تحتوي على عنصر رتبته هي المضاعف المشترك الأصغر للعددين n,m .

٢٦**- إذا كانت زمرة إبدالية تحتوي على زمرتين جزئيتين رتبتاهما n,m على الترتيب. أثبت أن هذه الزمرة تحتوي على زمرة جزئية رتبتها هي المضاعف المشترك الأصغر للعددين n,m (لا تقلق إن لم تستطع حل هذه المسألة باستخدام المعلومات التي عرفتها حتى الآن من نظرية الزمر. فحتى الآن لم يستطع أحد بما في ذلك نفسي حل هذه المسألة باستخدام المادة التي درست في هذه المرحلة من هذا الكتاب ولكن من الواجب أن تحاول ذلك. إن لدي مراسلات حول هذه المسألة أكثر من أية نقطة أخرى في هذا الكتاب).

٢٧- أثبت أن أية زمرة جزئية من زمرة دورية هي دورية.

٢٨- كم مولد يوجد للزمرة الدورية التي رتبتها n ؟ (يكون العنصر $b \in G$ مولدا إذا كان $(b)=G$).

لتكن U_n هي مجموعة الأعداد الصحيحة والأولية بالنسبة إلى n مع عملية الضرب قياس n . لقد سبق وأن اتضح في المسألة ١٥(ب) في المسائل التابعة للبند (٢-٣) أن U_n تكوِّن زمرة. وفي المسائل القليلة القادمة سنلقي نظرة على طبيعة U_n كزمرة وذلك لبعض القيم المعيَّنة للعدد n .

٢٩- أثبت أن U_8 ليست زمرة دورية.

٣٠- أثبت أن U_9 زمرة دورية. ما هي كل مولِّداتها؟

٣١- أثبت أن U_{17} زمرة دورية. ما هي كل مولِّداتها؟

٣٢- أثبت أن U_{18} زمرة دورية.

٣٣- أثبت أن U_{20} ليست زمرة دورية.

٣٤- أثبت أن كلا من U_{25}, U_{27} زمرة دورية.

٣٥- خَمِّنْ لأية قيمة من قيم n تجعل من U_n دورية (تستطيع التحقق من تخمينك بالرجوع إلى أي كتاب مناسب في نظرية الأعداد).

٣٦- إذا كان $a \in G$ و $a^m=e$ فأثبت أن $o(a)|m$.

٣٧- إذا تحققت العلاقتان $a^5=e$ و $aba^{-1}=b^2$ في الزمرة G حيث b,a عنصران من G فأوجد $o(b)$.

٣٨*- لتكن G زمـرة إبدالية منتهية بحيث يكون عدد حلول المعادلة $x^m=e$ في G هو على الأكثر n ، لكل عدد صحيح موجب n . أثبت أن G يجب أن تكون دورية .

٣٩- لتكن G زمرة و B,A زمرتين جزئيتين من G . إذا كان y,x عنصرين من G فلنعرف $x \sim y$ إذا كان $y=axb$ حيث $a \in A$ و $b \in B$. أثبت أن :

ا) العلاقة المعرفة آنفا هي علاقة تكافؤ.

ب) فصل التكافؤ للعنصر x هو

$$AxB = \{axb \mid a \in A, b \in B\}$$

(يطلق على المجموعة AxB **المجموعة المشاركة المزدوجة** (Double Coset) لكل من B,A في G .

٤٠- إذا كانت G زمرة منتهية فأثبت أن عدد العناصر في المجموعة المشاركة المزدوجة AxB هو

$$\frac{o(A)\,o(B)}{o(A \cap xBx^{-1})}$$

٤١- إذا كانت G زمرة منتهية وكانت A زمرة جزئية من G بحيث إن كل المجموعات المشاركة المزدوجة AxA تحتوي على العدد نفسه من العناصر فأثبت أن $gAg^{-1}=A$ لكل $g \in G$.

(٢-٦) الزمر الجزئية الناظمية والزمر الخارجة

لتكن G هي الزمرة S_3 و H هي الزمرة الجزئية $\{e,\phi\}$. لما كان دليل H في G يساوي 3 ، لذلك فإنه توجد ثلاث مجموعات مشاركة يمنى لـ H في G وكذلك توجد ثلاث مجموعات مشاركة يسرى ولنكتب هذه المجموعات كما يلي :

المجموعات المشاركة اليمنى	المجموعات المشاركة اليسرى
$H = \{e,\phi\}$	$H = \{e,\phi\}$
$H\psi = \{\psi, \phi\psi\}$	$\psi H = \{\psi, \psi\phi = \phi\psi^2\}$
$H\psi^2 = \{\psi^2, \phi\psi^2\}$	$\psi^2 H = \{\psi^2, \psi^2\phi = \phi\psi\}$

نلاحظ هنا حقيقة واضحة هي أن المجموعة المشاركة اليمنى $H\psi$ **ليست مجموعة** مشاركة يسرى. وبالتالي، فإنه بالنسبة لهذه الزمرة، على الأقل، ليس من الضروري أن تتطابق فكرتا المجموعتين المشاركتين اليمنى واليسرى.

لنعتبر مرة أخرى الزمرة $G=S_3$ ولنفرض أن N هي الزمرة الجزئية $\{e,\psi,\psi^2\}$. لما كان دليل N في G يساوي 2 ، لذلك فإنه توجد مجموعتان مشاركتان يُمنيان ومجموعتان مشاركتان يسريان لـ N في G يمكن كتابتهما كما يلي:

المجموعات المشاركة اليمنى	المجموعات المشاركة اليسرى
$N=\{e, \psi, \psi^2\}$	$N=\{e, \psi, \psi^2\}$
$N\phi=\{\phi, \psi\phi, \psi^2\phi\}$	$\phi N=\{\phi, \phi\psi, \phi\psi^2\}$
	$=\{\phi, \psi^2\phi, \psi\phi\}$

نلاحظ هنا أن كل مجموعة مشاركة يسرى لـN في G هي مجموعة مشاركة يمنى والعكس صحيح. وهكذا نرى تطابق المجموعات المشاركة اليسرى مع اليمنى لبعض الزمر الجزئية بينما لا تتطابق لبعض الزمر الجزئية الأخرى. إن الفضل يعود إلى عبقرية **جالوا** (Galois) لأنه هو الذي أدرك أن الزمرة الجزئية التي من أجلها تتطابق المجموعات المشاركة اليسرى مع اليمنى هي زمرة جزئية مميزة. وغالبا ما تكون المشكلة في

الرياضيات في القدرة على إدراك واكتشاف مفاهيم وثيقة الصلة ببعضها وعندما ينجز مثل هذا العمل فإننا نكون قد أنهينا معظم ما ننشده.

سنُعرِّف هذا النوع الخاص من الزمر الجزئية بطريقة مختلفة قليلا وسنثبت، عندئذ، أنها مكافئة للملاحظات في الفقرات السابقة.

تعريف

*يقال عن الزمرة الجزئية N من G **إنها زمرة جزئية ناظمية** **(Normal subgroup)** من G إذا كان $gng^{-1} \in N$ لكل g في G ولكل n في N.*

بعبارة أخرى مكافئة، يمكننا القول إنه إذا كانت gNg^{-1} هي المجموعة التي عناصرها من الصيغة gng^{-1} حيث $n \in N$ فإن N تكون زمرة جزئية ناظمية في G إذا وفقط إذا كان $gNg^{-1} \subset N$ لكل $g \in G$.

تمهيدية (٢-٦-١)

*تكون N زمرة جزئية ناظمية في G **إذا وفقط إذا كان** $gNg^{-1}=N$ لكل $g \in G$.*

البرهان

إذا كانت $gNg^{-1}=N$ لكل $g \in G$، فإنه بالتأكيد نجد أن $gNg^{-1} \subset N$ ومن ثم فإن N ناظمية في G.

لنفرض الآن أن N ناظمية في G. فإذا كان $g \in G$ فإن $gNg^{-1} \subset N$، كذلك نجد أن $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N$ الآن لما كان $g^{-1}Ng \subset N$ وكان $N=g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$ فإنه بناءً عليه يكون $N=gNg^{-1}$.

إننا نؤكد هنا على أن التمهيدية (٢-٦-١) لا تعني أن $gng^{-1} = n$ لكل $n \in N$ و $g \in G$. إن هذا قد لا يكون صحيحا. خذ على سبيل المثال الزمرة $G=S_3$ و N هي الزمرة

الجزئية $\{e, \psi, \psi^2\}$. بحساب $\phi N\phi^{-1}$ نجد أنها تساوي $\{e,\phi\psi\phi^{-1},\phi\psi^2\phi^{-1}\}=\{e,\psi^2,\psi\}$ ومع ذلك فإن $\phi\psi\phi^{-1}\neq\psi$. إن كل ما نريده هنا هو أن تكون مجموعة العناصر في gNg^{-1} هي نفسها مجموعة العناصر في N . نعود الآن إلى السؤال المتعلق بمساواة المجموعات المشاركة اليسرى واليمنى.

تمهيدية (٢-٦-٢)

تكون الزمرة الجزئية N في G زمرة جزئية ناظمية في G إذا وفقط إذا كانت كل مجموعة مشاركة يسرى هي مجموعة مشاركة يمنى لـ N في G .

البرهان

لنفرض أن N هي زمرة جزئية ناظمية في G . عندئذ $gNg^{-1}=N$ لكل $g\in G$ ، ومن ثم فإن $(gNg^{-1})g=Ng$ أي أن $gN=Ng$ ، وبالتالي فإن المجموعة المشاركة اليسرى gN هي المجموعة المشاركة اليمنى Ng .

ومن ناحية أخرى، لنفرض أن كل مجموعة مشاركة يسرى لـ N في G هي مجموعة مشاركة يمنى. أي أن المجموعة gN ، لكونها مجموعة مشاركة يسرى، يجب أن تكون مجموعة مشاركة يمنى، حيث $g\in G$.

ماذا يمكن أن تكون المجموعة المشاركة اليمنى؟

بما أن $g=ge\in gN$ فإنه مهما تكن المجموعة المشاركة اليمنى التي تساوي gN ، فإنها يجب أن تحتوي على العنصر g ، ولكن العنصر g ينتمي إلى المجموعة المشاركة اليمنى Ng . كذلك فإن المجموعتين المشاركتين اليمنيين لا تحتويان على عناصر مشتركة (تذكر برهان مبرهنة لاجرانج) وبناءً عليه، فإن هذه المجموعة المشاركة اليمنى وحيدة، أي أن $gN=Ng$ ، وبعبارة أخرى، $gNg^{-1}=Ngg^{-1}=N$ أي أن N زمرة جزئية ناظمية.

لقد عرفنا سابقا ما هو المقصود بالمجموعة HK حيث K,H زمرتان جزئيتان من G . وبإمكاننا أن نوسع هذا التعريف إلى مجموعات جزئية اختيارية كما يلي:

إذا كانت B,A مجموعتين في الزمرة G فإن $AB=\{x\in G|x=ab,a\in A,b\in B\}$.
ماذا يمكن أن نقول عندما $A=B=H$ حيث H زمرة جزئية من G ؟

إن الجواب على ذلك هو أن $HH=\{h_1h_2 \mid h_1, h_2\in H\}\subset H$ لأن H مغلقة بالنسبة لعملية الضرب ولكن $HH\supset He\supset H$ ، لأن $e\in H$ ، وهكذا فإن $HH=H$.

لنفـرض الآن أن N زمـرة جزئية ناظمية من G وأن $a,b\in G$ ولنعتبر $(Na)(Nb)$ ؛ إن $aN=Na$ لأن N ناظمية في G وبالتالي فإن

$$NaNb = N\,(aN)\,b = N\,(Na)\,b = NNab = Nab$$

كم هي كثيرة تلك الإمكانات التي يمكن أن تزودنا بها هذه الصيغة البسيطة! لكن قبل أن نستمر في الموضوع فإننا نسجلها وذلك للتأكيد والرجوع إليها.

تمهيدية (٢-٦-٣)

تكـون الـزمرة الجزئية N في G ناظمية في G إذا وفقط إذا كان حاصل ضرب مجموعتين مشاركتين يمنيين لـ N في G هي مجموعة مشاركة يمنى لـ N في G .

البرهان

لقـد برهنا آنفا أنه إذا كانت N ناظمية في G ، فإن حاصل ضرب مجموعتين مشاركتين يمنيين لـ N في G هي مجموعة مشاركة يمنى لـ N في G . إن برهان النصف الثاني من التمهيدية هو أحد المسائل الواردة في نهاية هذا البند.

لنفرض الآن أن N ناظمية في G . إن الصيغة $NaNb=Nab$ تبدو طبيعية ؛ أي أن حاصل ضرب مجموعتين مشاركتين يمنيين هي مجموعة مشاركة يمنى.

هل بإمكاننا استخدام هذا الضرب لتحويل مجموعة المجموعات المشاركة اليمنى إلى زمرة؟ بالتأكيد يمكن أن نفعل ذلك.

إن هذا النوع من البناء الذي غالبا ما يحدث في الرياضيات له أهمية بالغة وغالبا ما ندعوه **بالبناء الخارج** (Quotient structure) . لنجعل G/N ترمز إلى مجموعة المجموعات المشاركة اليمنى لـ N في G [أي أن عناصر G/N هي مجموعات جزئية محددة في G] .

إننا ندعي أن ضرب المجموعات المشاركة اليمنى يحقق ما يلي :

١) إذا كان $X, Y \in G/N$ فإن $XY \in G/N$ ، لأنه إذا كان $X=Na$ و $Y=Nb$ ، حيث b,a عنصران من G فإن $XY=NaNb=Nab \in G/N$.

٢) إذا كان $X,Y,Z \in G/N$ فإن $XY=Na, Y=Nb, Z=Nc$ حيث $a,b,c \in G$ ، وبناءً عليه فإن :

$$(XY)Z=(NaNb)Nc=N(ab)Nc=N(ab)c=Na(bc)$$

$$= NaNbc=Na(NbNc)=X(YZ)$$ (لأن G تجميعية)

لذا فإن الضرب في G/N يحقق خاصة التجميع .

٣) لنعتبر العنصر $N=Ne \in G/N$ ، فإذا كان $X \in G/N$ فإن $X=Na$ حيث $a \in G$ ومن ثم فإن

$$XN = NaNe = Nae = Na = X$$

وبالمثل فإن $NX=X$ ، أي أن Ne هو العنصر المحايد في G/N .

٤) لنفرض أن $X=Na \in G/N$ (حيث $a \in G$) ؛ وعليه فإن $Na^{-1} \in G/N$ ، كما أن $NaNa^{-1} = Naa^{-1}=Ne$ وبالمثل فإن $Na^{-1}Na=Ne$ ، أي أن Na^{-1} هو معكوس العنصر Na في G/N . ولكن النظام الذي يحقق ١ ، ٢ ، ٣ ، ٤ هو ذلك النظام الذي ندعوه زمرة . أي أن :

مبرهنة (٢-٦-١)

إذا كانت G زمرة و N زمرة جزئية ناظمية في G فإن G/N زمرة أيضا . وتدعى هذه الزمرة بالزمرة الخارجة Quotient group أو زمرة العامل (Factor group) للزمرة G على N .

إذا كانت G ، بالإضافة إلى ذلك، زمرة منتهية فما هي رتبة G/N ؟ لما كانت عناصر G/N هي المجموعات المشاركة اليمنى لـ N في G ولما كان عدد هذه المجموعات هو $i_G(N) = \frac{o(G)}{o(N)}$ فإنه يمكننا أن نقول:

تمهيدية (٢-٦-٤)

إذا كانت G زمرة منتهية و N زمرة جزئية ناظمية في G فإن $o(G/N) = \frac{o(G)}{o(N)}$

ونختتم هذا البند بهذا المثال

لتكن G زمرة الأعداد الصحيحة بالنسبة لعملية الجمع ولتكن N هي مجموعة مضاعفات العدد 3 . لما كانت العملية المعرفة على G هي الجمع، لهذا فإننا سنكتب المجموعات المشاركة لـ N في G على الصيغة N+a بدلا من Na . لنعتبر الآن المجموعات المشاركة الثلاث N+2, N+1, N . إننا ندعي أن هذه المجموعات المشاركة هي كل المجموعات المشاركة لـN في G ، لأنه إذا كان $a \in G$ فإن $a=3b+c$ ، حيث $b \in G$ و c هو صفر أو 1 أو 2 [أي أن c هو باقي قسمة a على 3] وهكذا فإن $N+a=N+3b+c=(N+3b)+c=N+c$ لأن $3b \in N$. أي أن كل مجموعة مشاركة، كما أشرنا إلى ذلك، هي واحدة من المجموعات N+2, N+1, N ، أي أن:

$$G/N = \{N, N+1, N+2\}$$

الآن كيف نجمع العناصر في G/N ؟

يمكن ترجمة العلاقة NaNb = Nab إلى:

$$(N+1) + (N+2) = N + 3 = N \ (3 \in N \text{ لأن})$$

و $(N+2) + (N+2) = N+4 = N+1$ وهلم جرا. ومن السهل أن يشعر القارىء أن للزمرة G/N علاقة قريبة بزمرة الأعداد الصحيحة قياس 3 ، بالنسبة لعملية الجمع. وواضح أن ما عملناه بالنسبة للعدد 3 يمكن عمله لأي عدد صحيح، وعلى أية حال، فإن الزمرة الخارجة في هذه الحالة توحي بعلاقة مع مجموعة الأعداد الصحيحة قياس n بالنسبة للجمع وهذا النوع من العلاقة سيوضح في البند التالي.

مسـائـل

١ ـ إذا كانت H زمرة جزئية من G بحيث يكون حاصل ضرب مجموعتين مشاركتين يمنيين لـH في G هي مجموعة مشاركة يمنى لـH في G فأثبت أن H ناظمية في G .

٢ ـ إذا كانت G زمرة و H زمرة جزئية من G بحيث يكون دليل H في G يساوي 2 فأثبت أن H ناظمية في G .

٣ ـ إذا كانت N زمرة جزئية ناظمية في G وكانت H هي أية زمرة جزئية في G فأثبت أن NH زمرة جزئية في G .

٤ ـ أثبت أن تقاطع أي زمرتين جزئيتين ناظميتين في G هي زمرة جزئية ناظمية في G .

٥ ـ إذا كانت H زمرة جزئية في G وكانت N زمرة جزئية ناظمية في G فأثبت أن $H \cap N$ زمرة جزئية ناظمية في H .

٦ ـ أثبت أن أية زمرة جزئية من زمرة إبدالية هي ناظمية .

٧* ـ هل عكس مسألة ٦ صحيح؟ إذا كانت الإجابة بنعم فأثبت ذلك . وإذا كانت خلاف ذلك فأورد مثالا لزمرة غير إبدالية بحيث تكون جميع زمرها الجزئية ناظمية .

٨ ـ أورد مثالا لزمرة G تحتوي على زمرة جزئية H ولعنصر $a \in G$ بحيث يكون $aHa^{-1} \subset H$ ولكن $aHa^{-1} \neq H$.

٩ ـ افرض أن H هي الزمرة الجزئية الوحيدة في زمرة منتهية G التي رتبتها $o(H)$. أثبت أن H زمرة جزئية ناظمية في G .

١٠ ـ إذا كانت H زمرة جزئية في G و $N(H) = \{g \in G | gHg^{-1} = H\}$ فأثبت أن

(ا) $N(H)$ زمرة جزئية من G

(ب) H ناظمية في $N(H)$

(جـ) إذا كانت H زمرة جزئية ناظمية في الزمرة الجزئية K حيث K زمرة جزئية من G فإن $K \subset N(H)$ [أي أن: $N(H)$ هي أكبر الزمر الجزئية في G بحيث تكون H ناظمية فيها] .

(د) H ناظمية في G إذا وفقط إذا كان $N(H) = G$

١١ ـ إذا كانت M, N زمرتين جزئيتين ناظميتين في G فأثبت أن NM هي زمرة جزئية ناظمية في G .

١٢* ـ إذا كانت M, N زمرتين جزئيتين ناظميتين في G بحيث يكون $N\cap M=(e)$.
فأثبت أنه لأي n في N و m في M يكون $mn=nm$.

١٣ ـ إذا كانت الزمرة الجزئية الدورية T في G ناظمية .
فأثبت أن كل زمرة جزئية من T هي ناظمية في G .

١٤* ـ أورد مثـالا تثبـت فيـه أنـه يمكن إيجـاد ثـلاث زمـر E, F, G بحيث إن $E\subset F\subset G$, E ناظمية في F, F ناظمية في G لكن E ليست ناظمية في G .

١٥ ـ إذا كانت N ناظمية في G وكان $a\in G$.
فأثبت أن رتبة a تقبل القسمة على رتبة العنصر Na في G/N .

١٦ ـ إذا كانت N زمـرة جزئية ناظمية في الـزمـرة المنتهية G بحيث يكـون $i_G(N)$ و $o(N)$ أوليين نسبيا .
فأثبت أن كل عنصر $x\in G$ يحقق العلاقة $x^{o(N)}=e$ يجب أن يكون في N .

١٧ ـ لنعرف G على أنها جميع الرموز x^iy^j , $i=0,1$, $j=0,1,\ldots,n-1$ حيث نفرض أن $x^iy^j = x^{i'}y^{j'}$ إذا وفقط إذا كان $i=i'$, $j=j'$ ، $x^2=y^n=e$ ، $n>2$, $xy = y^{-1}x$.

(ا) أوجد صيغة الضرب $(x^iy^j)(x^ly^k)$ على الصورة $x^\alpha y^\beta$.

(ب) باستخدام هذا الضرب أثبت أن G زمرة غير إبدالية رتبتها 2n .

(جـ) إذا كان n فرديا فأثبت أن مركز G هو (e) بينما إذا كان n زوجيا فإن مركز G أكبر من (e) .

إن هذه الزمرة تسمى بالزمرة **الزوجية** (Dihedral) وإن التصور الهندسي لهذه الزمرة هو كما يلي :

لنفرض أن y تمثل دوران المستوى الإقليدي حول نقطة الأصل بزاوية مقدارها $\frac{2\pi}{n}$ وأن x تمثل الانعكاس حول المحور الرأسي، عندئذ تكون G في هذه الحالة هي زمرة حركات المستوى المولدة بكل من x و y .

١٨ ـ لتكن G هي الـزمـرة التي تتحقق فيهـا العـلاقـة $(ab)^n=a^nb^n$ ، لكل b,a في G ، حيث n عدد صحيح أكبر من 1 .

أثبت أن

(أ) $G^{(n)}=\{x^n|x\in G\}$ زمرة جزئية ناظمية في G.

(ب) $G^{(n-1)}=\{x^{n-1}|x\in G\}$ زمرة جزئية ناظمية في G.

١٩ - لتكن G هي الزمرة الواردة في المسألة (١٨)، أثبت أن

(أ) $a^{n-1}b^n = b^na^{n-1}$ لكل b,a في G.

(ب) $(a\,b\,a^{-1}b^{-1})^{n(n-1)}=e$ لكل b,a في G.

٢٠ - لتكن G هي الزمرة التي يكون فيها $(ab)^p = a^pb^p$ لكل b,a في G ، حيث p عدد أولي ولتكن S هي المجموعة $\{x\in G|x^{p^m}=e\}$ حيث m عدد ما يعتمد على x. أثبت أن

(أ) S زمرة جزئية ناظمية في G .

(ب) إذا كانت $\bar{G}=G/S$ وكان $\bar{x}\in\bar{G}$ يحقق الشرط $\bar{x}^p=e$ فإن $\bar{x}=\bar{e}$.

٢١* - لتكن G هي مجموعة المصفوفات من النوع 2x2 من الصيغة $\binom{a\ b}{0\ d}$ على مجموعة الأعداد الحقيقية، حيث $ad\neq0$ بالنسبة، لعملية ضرب المصفوفات. ولتكن $N=\{\binom{1\ b}{0\ 1}\}$ ، أثبت أن

(أ) N زمرة جزئية ناظمية في G

(ب) G/N زمرة إبدالية.

(٢-٧) التشاكلات

إن الأفكار والنتائج الواردة في هذا البند تتداخل مع مثيلاتها في البند السابق، وإن وجدت فكرة مركزية مشتركة لجميع مواضيع الجبر الحديث فهي فكرة التشاكل ويمكن أن نُعرِّفها بأنها تطبيق من نظام جبري إلى نظام جبري مشابه، يحافظ على البنية الجبرية. سنُعَرِّف التشاكلات بصورة أدق بالنسبة للزمر.

تعريف

*يقال عن التطبيق ϕ من الزمرة G إلى الزمرة $\bar{G}$ إنه **تشاكل** (Homomorphism) إذا كان $\phi(ab) = \phi(a)\phi(b)$ لكل b,a في G .*

لاحظ أن حاصل الضرب ab في الحد $\phi(ab)$ في الطرف الأيسر ينتمي إلى G وذلك باستخدام الضرب في G ، بينما يكون $\phi(a)\phi(b)$ في الطرف الأيمن هو حاصل ضرب عناصر محسوبا في $\bar{G}$.

مثال (٢ ـ ٧ ـ ١)

إن $\phi(x) = e$ لكل $x \in G$ هو تشاكل من G إلى نفسها وكذلك الحالة بالنسبة للتطبيق $\phi(x)=x$ لكل $x \in G$.

مثال (٢ ـ ٧ ـ ٢)

لتكن G هي زمرة الأعداد الحقيقية بالنسبة لعملية الجمع (ab هنا يعني العدد الحقيقي $a+b$ لكل b,a في G) ولتكن $\bar{G}$ هي زمرة الأعداد الحقيقية غير الصفرية بالنسبة لعملية الضرب العادية ولنعرف $\phi: G \to \bar{G}$ بالقاعدة $\phi(a) = 2^a$.

لكي نتحقق من أن هذا التطبيق هو تشاكل يجب علينا أن نتأكد من أن $\phi(ab)=\phi(a)\phi(b)$ ، حيث يعني الضرب في الطرف الأيسر العملية المعرفة على G (أي عملية الجمع)، وبعبارة أخرى، يجب أن نتأكد من أن $2^{a+b}=2^a.2^b$ والذي هو صحيح بالفعل. ولما كان 2^a دائما موجبا، فإن صورة ϕ ليست كل $\bar{G}$ ، مما يعني أن ϕ تشاكل من G إلى $\bar{G}$ ، ولكنه ليس غامرا .

مثال (٢ ـ ٧ ـ ٣)

لتكن $G=\{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$ و $\bar{G} = \{e, \phi\}$ ولنُعَرِّف التطبيق $f: G \to \bar{G}$ وفق القاعدة

$$f(e) = e, f(\phi) = \phi, f(\psi) = e, f(\psi^2) = e, f(\phi\psi) = \phi, f(\phi\psi^2) = \phi$$

إن على القارىء التحقق من أن f المعرف آنفا هو تشاكل .

مثال (٢ ـ ٧ ـ ٤)

لنفرض أن G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع وأن $G=\bar{G}$ ولنعرف ϕ بالقاعدة $\phi(x)=2x$ لكل $x \in G$ ، عندئذ فإن ϕ تشاكل لأن

$$\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$$

مثال (٢ ـ ٧ ـ ٥)

لنفرض أن G هي زمرة الأعداد الحقيقية باستثناء الصفر وذلك بالنسبة لعملية الضرب، $\bar{G}=\{1,-1\}$ حيث يكون:

$$1.1 = 1, (-1)(-1) = 1, 1(-1) = (-1)1 = -1$$

ولنُعرِّف $\phi: G \to \bar{G}$ وفق العلاقة:

$$\phi(x) = \begin{cases} 1 & \text{إذا كان } x \text{ موجبا} \\ -1 & \text{إذا كان } x \text{ سالبا} \end{cases}$$

إن كون ϕ تشاكلا يكافىء العبارات:

موجب × موجب = موجب، موجب × سالب = سالب، سالب × سالب = موجب

مثال (٢ ـ ٧ ـ ٦)

لنفرض أن G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع وأن $\bar{G}_n$ هي زمرة الأعداد الصحيحة مقياس n بالنسبة لعملية الجمع المُعَرَّفة عليها ولنُعَرِّف ϕ من G إلى $\bar{G}_n$ كما يلي: $\phi(x)$ يساوي باقي قسمة x على n . إنه يمكن للقارىء أن يتأكد، وبسهولة، من أن ϕ تشاكل.

مثال (٢ ـ ٧ ـ ٧)

لنفرض أن G هي زمرة الأعداد الحقيقية الموجبة بالنسبة لعملية الضرب وأن $\bar{G}$ هي زمرة الأعداد الحقيقية بالنسبة لعملية الجمع.

ولنُعَرِّف $\phi: G \to \bar{G}$ وفق العلاقة $\phi(x) = \log_{10}x$

عندئذ

$$\phi(xy) = \log_{10}(xy) = \log_{10}x + \log_{10}y = \phi(x) + \phi(y)$$

لأن العملية في الطرف الأيمن هي العملية المعرفة على $\bar{G}$ وهي عملية الجمع. وبالتالي

فإن ϕ تشـاكل من G إلى $\bar{G}$. إنه ليس تشاكلا فحسب، بل هو بالإضافة إلى ذلك أحادي وغامر أيضا.

*** مثال (٢ - ٧ - ٨)**

لنفـرض أن G هي زمرة المصفوفات $\binom{a\ b}{c\ d}$ من النوع 2×2 على مجموعة الأعداد الحقيقية بحيث يكون ad−bc≠0 بالنسبة لعملية ضرب المصفوفات.

ولنفرض أن $\bar{G}$ هي زمرة الأعداد الحقيقية باستثناء الصفر بالنسبة لعملية الضرب ولنُعَـرِّف $\phi:G \to \bar{G}$ وفق العلاقة : $\phi\binom{a\ b}{c\ d} = ad-bc$ عندئذ فإن ϕ تشاكل من G على $\bar{G}$ (تحقق من ذلك).

إن التمهيدية الآتية، تمدنا بصنف غير منتهٍ من أمثلة التشاكلات. وعندما نثبت المبرهنة (٢-٧-١) فإنه ستُظْهِر لنا، إن هذا الصنف يمثل من وجهة نظر معيّنة، أعم حالات التشاكل.

تمهيدية (٢-٧-١)

لنفرض أن G زمرة و N زمرة جزئية ناظمية فيها ولْنُعَرِّف التطبيق ϕ من G إلى G/N كما يلي $\phi(x) = Nx$ لكل $x \in G$ عندئذ يكون ϕ تشاكلاً من G على G/N .

البرهـــان

في الحقيقة، لا يوجد شيء يستدعي البرهان هنا، لأننا قد برهنا على هذه الحقيقة مرات عديدة. ولكننا نعيده هنا للتأكيد.

إن من الـواضح أن ϕ غامر لأن كل عنصر $X \in G/N$ هو من الصيغة $X=Ng$ حيث $g \in G$ وهذا يعني أن $X=\phi(g)$.

ولإثبات أن ϕ تشاكل يجب التحقق من خاصية الضرب وذلك بملاحظة أنه إذا كان $x,y \in G$ فإن :

$$\phi(xy) = Nxy = NxNy = \phi(x)\,\phi(y)$$

إن التمهيدية (٢-٧-١) والمثـال السابق لها يؤكدان حقيقة مهمة هي أنه ليس ضروريا أن يكـون كل تشـاكـل أُحـاديا. ولكنـه يوجد نسق معيّن في هذه الطريقة للانحراف عن الأُحادية. وسيصبح هذا واضحا في السطور القليلة الآتية.

تعريف

*إذا كان ϕ تشـاكـلا من G إلى $\bar{G}$ فإننـا نعـرف **نواة** ϕ(Kernel) والتي نرمز لها بالرمز K_ϕ بأنها*

$$K_\phi = \{x \in G \mid \phi(x) = \bar{e}\}$$

حيث $\bar{e}$ هو العنصر المحايد في $\bar{G}$.

من المستحسن أن نبرهن على أن K_ϕ ليست مجموعة خالية وذلك قبل البحث عن أية خاصة لها وهذا ما سنتناوله في الجزء الأول من التمهيدية الآتية.

تمهيدية (٢-٧-٢)

إذا كان ϕ تشاكلا من G إلى $\bar{G}$ فإن:

(١) $\phi(e) = \bar{e}$ *هو العنصر المحايد في* $\bar{G}$.

(٢) $\phi(x^{-1}) = \phi(x)^{-1}$ *لكل* $x \in G$.

البرهان

لبرهان (١) نحسب الآتي:

$$\phi(x)\,\bar{e} = \phi(x) = \phi(xe) = \phi(x)\,\phi(e)$$

واستنادا إلى خاصة الاختزال في $\bar{G}$ نحصل على $\phi(e)=\bar{e}$.

لبرهان (٢) نلاحظ أن:

$$\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\,\phi(x^{-1})$$

ومن تعريف $\phi(x)^{-1}$ في $\bar{G}$ نحصل على النتيجة المطلوبة، أي أن $\phi(x^{-1}) = \phi(x)^{-1}$.

إن برهان التمهيدية (٢-٧-٢) لابد أن يُذَكِّر القارىء الذي سبق له دراسة اللوغاريتمات ببرهان نتائج مماثلة مثل $\log 1=0$ و $\log \frac{1}{x} = -\log x$. إن هذا ليس من قبيل المصادفة ذلك لأن التطبيق $\phi: x \to \log x$ هو تشاكل من زمرة الأعداد الحقيقية الموجبة بالنسبة لعملية الضرب إلى زمرة الأعداد الحقيقية بالنسبة لعملية الجمع، كما رأينا ذلك في المثال (٢-٧-٧).

إن تمهيدية (٢-٧-٢) تثبت لنا أن العنصر المحايد e ينتمي إلى نواة أي تشاكل وبناءً عليه فإن النواة غير خالية. وبإمكاننا الحصول على معلومات أكثر من ذلك حيث نجد:

تمهيدية (٢-٧-٣)

إذا كانت K هي نواة التشاكل ϕ من G إلى $\bar{G}$ فإن K زمرة جزئية ناظمية في G .

البرهان

أولا: يجب أن نثبت أن K هي زمرة جزئية من G ولكي يتم ذلك، يجب أن نثبت أن K مغلقة بالنسبة للضرب وأنها تحتوي على معكوس أي عنصر في K .

إذا كان $x, y \in K$ فإن $\phi(x) = \bar{e}$ و $\phi(y) = \bar{e}$ ، حيث $\bar{e}$ هو العنصر المحايد في $\bar{G}$.

ومن ثم فإن $\phi(xy) = \phi(x)\,\phi(y) = \bar{e}\,\bar{e} = \bar{e}$ أي أن $xy \in K$.

أيضا إذا كان $x \in K$ فإن $\phi(x) = \bar{e}$ ، واستنادا إلى تمهيدية (٢-٧-٢) يكون $\phi(x^{-1}) = \phi(x)^{-1} = \bar{e}^{-1} = \bar{e}$ أي أن $x^{-1} \in K$ وعليه فإن K زمرة جزئية من G .

لبرهان ناظمية K ، يجب علينا أن نثبت أنه لأي $g \in G$ و $k \in K$ يكون $gkg^{-1} \in K$ ، بعبارة أخرى، يجب أن نثبت أنه متى ما كان $\phi(k) = \bar{e}$ فإن $\phi(gkg^{-1}) = \bar{e}$. ولكن

$$\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi((g^{-1}) = \phi(g)\,\bar{e}\phi(g)^{-1} = \phi(g)\,\phi(g)^{-1} = \bar{e}$$

بهذا ينتهي برهان التمهيدية (٢-٧-٣).

لنفرض الآن أن ϕ تشاكل من الزمرة G على الزمرة $\bar{G}$ وأن K هي نواة ϕ . فإذا كان $\bar{g} \in \bar{G}$ فإننا نقول إن العنصر $x \in G$ صورة عكسية للعنصر $\bar{g}$ تحت تأثير ϕ إذا كان $\phi(x)=\bar{g}$.

ولنسأل: ما هي الصورة العكسية للعنصر $\bar{g}$ ؟
إذا كان $\bar{g} = \bar{e}$ فإن الجواب واضح وهو K (من تعريف K). والآن ماذا لو كان $\bar{g} \neq \bar{e}$ ؟ حسنا لنفرض أن $x \in G$ هو إحدى الصور العكسية للعنصر $\bar{g}$.
هل يمكن الحصول على عناصر أخرى؟ إن الجواب، بكل وضوح، نعم، لأنه إذا كان $k \in K$ وكان $y=kx$ فعندئذ

$$\phi(y) = \phi(kx) = \phi(k)\,\phi(x) = \bar{e}\,\bar{g} = \bar{g}$$

أي أن جميع عناصر المجموعة Kx تنتمي إلى الصورة العكسية للعنصر $\bar{g}$ متى ما كان x كذلك.

هل يمكن وجود عناصر أخرى؟
دعنا نفرض أن $\phi(z) = \phi(x)$ عندئذ $\phi(z) = \bar{e} = \phi(x)$ وهذا يقتضي أن يكون $\phi(z)\,\phi(x)^{-1} = e$ وحيث إن $\phi(x)^{-1} = \phi(x^{-1})$ لذلك فإن

$$\bar{e} = \phi(z)\,\phi(x)^{-1} = \phi(z)\,\phi(x^{-1}) = \phi(z\,x^{-1})$$

مما يعني أن $zx^{-1} \in K$ ، أي أن $z \in Kx$. بعبارة أخرى، نكون قد أثبتنا أن Kx هي بالضبط جيمع الصور العكسية للعنصر $\bar{g}$ متى كان x صورة عكسية له. بهذا نكون قد أثبتنا التمهيدية الآتية.

تمهيدية (٢-٧-٤)

إذا كان ϕ تشاكلا من الزمرة G على الزمرة $\bar{G}$ وكانت K هي نواة ϕ فإن مجموعة الصور العكسية للعنصر $\bar{g} \in \bar{G}$ تحت تأثير ϕ هي Kx حيث x هي أية صورة عكسية للعنصر $\bar{g}$ في $\bar{G}$.

حالة خاصة من هذه التمهيدية هي عندما $K=(e)$.

هنا، ووفقا لتمهيدية (٢-٧-٤) فإن أي عنصر $\bar{g}\in\bar{G}$ له صورة عكسية مكونة من عنصر واحد فقط، وهذا يعني أن ϕ تطبيق أحادي. والعكس صحيح، بمعنى أنه إذا كان التشاكل من G إلى $\bar{G}$ أحاديا (ليس من الضروري أن يكون غامرا) فإن نواته يجب أن تتكون من العنصر المحايد فقط.

تعريف

*يقال عن التشاكل ϕ من G إلى $\bar{G}$ إنه **تماثل** (isomorphism) إذا كان ϕ أحاديا.*

تعريف

*يقال عن الزمرتين G, G^* إنهما **متماثلتان** (isomorphic) إذا وجد تماثل من G على G^* وفي هذه الحالة نكتب $G\approx G^*$ ونترك للقارىء برهان الحقائق الثلاث الآتية:*

١ - $G \approx G$

٢ - إذا كانت $G \approx G^*$ فإن $G^* \approx G$

٣ - إذا كانت $G \approx G^*$ وكانت $G^* \approx G^{**}$ فإن $G \approx G^{**}$.

عندما تكون زمرتان متماثلتين فإنه يمكن اعتبارهما متساويتين إلى حد ما. إنهما يختلفان لأن عناصرهما مختلفة. وإذا عرفنا حسابات في زمرة معيّنة، فإن بوسعنا باستخدام التماثل إجراء حسابات مشابهة في الزمرة الأخرى.

يمكن تشبيه التماثيل بقاموس يُمكِّنُ إنسانًا من ترجمة عبارة في لغة ما إلى عبارة أخرى بالمعنى نفسه في لغة أخرى (لسوء الحظ، لا يوجد قاموس متكامل كهذا لأن الكلمات لا يكون لها معنى واحد في اللغات، كما أن المعاني لا تنقل من خلال ترجمة حرفية) ولكن مجرد القول بإمكانية التعبير عن جملة ما بلغة أخرى يعتبر ذا مردود قليل مما يجعل حاجتنا للقاموس ليقوم بمثل هذه الترجمة أمرا لا مفر منه. وبالمثل فإن معرفة أن زمرتين متماثلتان قد يعتبر ذا مردود قليل ولكن من الأهمية بمكان معرفة التماثل نفسه،

ولذلك عندما نبرهن على أن زمرتين هما زمرتان متماثلتان فإننا سنحاول إيجاد التطبيق المطلوب الذي يعطي التماثل بين الزمرتين.

ونعود الآن إلى تمهيدية (٢-٧-٤) حيث نجد فيها طريقة لمعرفة متى يكون التشاكل تماثلا وذلك بدلالة النواة.

نتيجة

إذا كان ϕ من G إلى $\bar{G}$ تشاكلا وكانت K_ϕ هي نواة ϕ فإن ϕ يكون تماثلا من G إلى $\bar{G}$ إذا وفقط إذا كانت $K_\phi=(e)$.

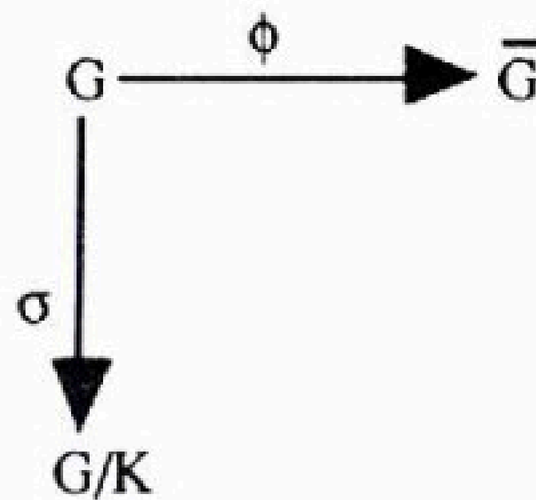
إن في هذه النتيجة طريقة قياسية لإثبات أن زمرتين متماثلتان أو لا ، نوجد تشاكلا من زمرة على أخرى ثم نثبت بعد ذلك أن نواة هذا التشاكل هي العنصر المحايد فقط. وستتضح لنا هذه الطريقة من برهان المبرهنة المهمة الآتية.

مبرهنة (٢-٧-١)

لنفرض أن ϕ تشاكل من G على $\bar{G}$ وأن نواته هي K . عندئذ $G/K \approx \bar{G}$.

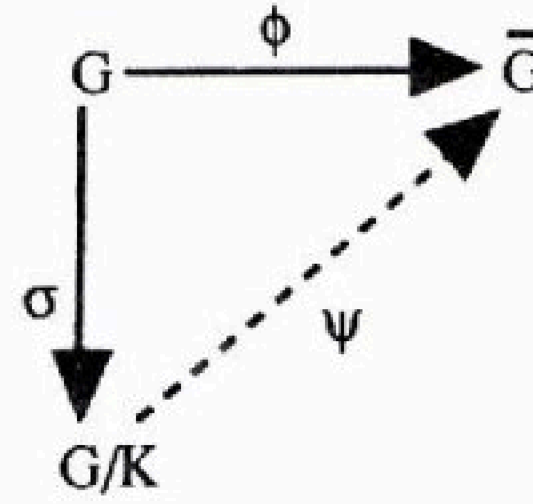
البرهان

لنعتبر الرسم:

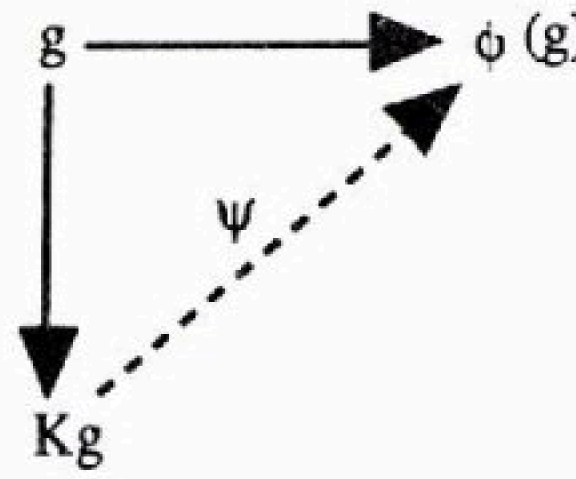


حيث $\sigma(g) = Kg$.

ونود إكمال الرسم السابق على النحو التالي:



من الـواضـح أنـه لكي ننشيء التطبيق ψ من G/K إلى $\bar{G}$ يجب أن تستخدم G كوسيط بحيث يكون هذا الإنشاء غير معقد نسبيا. يبدو أن الأمر الطبيعي هو أن نكمل الرسم السابق كما يلي:



بهذا التمهيد نُعـرِّفْ التـطبيق ψ من G/K إلى $\bar{G}$ وفقـا للقـاعدة: إذا كان $X\in G/K$ حيث $X=Kg$ فإن $\psi(X) = \phi(g)$. ومن حق القاريء أن يتساءل هل هذا التطبيق حسن التعريف؟

حسنـا. إذا كان $X\in G/K$ فإنه يمكن كتابته على الصيغة Kg بعدة طرق [على سبيل المثال $Kg=Kkg$ ، $k\in K$]؛ ولكن إذا كان $X=Kg=Kg'$ حيث $g,g'\in G$ فإننا نجد من ناحية أن $\psi(X)=\phi(g)$ ومن ناحية أخرى $\psi(X)=\phi(g')$ ولكي يكون للتطبيق معنى، فإنه يجب أن يكون $\phi(g)=\phi(g')$. لذلك: نفرض أن $Kg=Kg'$ ؛ $g=kg'$ حيث $k\in K$ وبناءً على ذلك،

$$\phi(g) = \phi(kg') = \phi(k)\,\phi(g') = \bar{e}\,\phi(g') = \phi(g')$$

لأن $k\in K$ ، حيث K هي نواة ϕ .

الآن نثبت أن ψ غامر فإذا كان $\bar{x}\in\bar{G}$ فإن $\bar{x}=\phi(g)$ ، حيث $g\in G$ (لأن ϕ غامر) وبـالتـالي فإن $\bar{x}=\phi(g)=\psi(Kg)$. إذا كان $X,Y\in G/K$ فإن $X=Kg$, $Y=Kf$ ، حيث $g, f\in G$ وعندئذ $XY=KgKf=Kgf$ ومن ثم فإن

$$\psi(XY) = \psi(Kgf) = \phi(gf) = \phi(g)\,\phi(f)$$

وذلك لأن ϕ تشاكل من G على $\bar{G}$. ولكن

$$\psi(Y) = \psi(Kf) = \phi(f) \ , \ \psi(X) = \psi(Kg) = \phi(g)$$

ولذلك فإن $\psi(XY) = \psi(X)\,\psi(Y)$ أي أن ψ تشاكل من G/K على $\bar{G}$.

لكي نثبت أن ψ تماثل من G/K على $\bar{G}$ يجب علينا أن نبين أن نواة ψ هي العنصر المحايد في G/K . ولما كان العنصر المحايد في G/K هو Ke=K لذا فإنه يجب علينا أن نثبت أنه إذا كان $\psi(Kg) = \bar{e}$ فإن Kg=Ke=K. إن من السهل إثبات هذا، لأنه إذا كان $\bar{e}=\psi(Kg)=\phi(g)$ ، فإن $\phi(g)=\bar{e}$. ومن ثم فإن g عنصر من نواة ϕ التي هي K . ولكن، عندئذ، Kg=K لأن K زمرة جزئية من G . وبضم هذه المعلومات مع بعضها نجد أننا قد أثبتنا وجود تشاكل أحادي من G/K على $\bar{G}$. وهكذا نجد أن $G/K \approx \bar{G}$. وبهذا نكون قد أثبتنا مبرهنة (٢-٧-١).

إن مبرهنة (٢-٧-١) مهمة، ذلك لأنها تفيدنا وبدقة عن الزمر التي يمكن أن تنشأ على هيئة صورة تشاكلية لزمرة معينة. إنه يمكن التعبير عن هذه الزمر على الصيغة G/K حيث K زمرة جزئية ناظمية من G . ولكن من تمهيدية (٢-٧-١) نجد أن G/N صورة تشاكلية للزمرة G حيث N زمرة جزئية ناظمية من G . وهكذا فإنه يوجد تقابل بين الصور التشاكلية للزمرة G والزمر الجزئية الناظمية فيها. وإذا أراد القارىء أن يبحث عن جميع الصور التشاكلية للزمرة G فإن بوسعه التوصل إلى ذلك بالعمل داخل الزمرة G وذلك كما يلي: أوجد جميع الزمر الجزئية الناظمية N في G ثم كون جميع الزمر G/N . إن مجموعة الزمر المكونة بهذه الطريقة هي جميع الصور التشاكلية للزمرة G [إلى حد التماثل].

يقال عن الزمرة G إنها زمرة **بسيطة** (Simple) إذا لم يكن لها صورة تشاكلية غير تافهة. وبعبارة أخرى، إذا كانت لا تحتوي على زمرة جزئية ناظمية غير تافهة.

هناك تخمين (حدس) مشهور بقي بدون برهان لمدة طويلة يقول إن رتبة أية زمرة بسيطة غير إبدالية ومنتهية هي عدد زوجي. لقد تم برهان هذا التخمين من قبل الرياضيين الأمريكيين **ولتر فايت** (Walter fiet) **وجون طومسون** (John Thompson) .

لقد أشرنا إلى أن مفهوم التشاكل هو مفهوم مهم جدا. لكي نُؤكِّد هذا القول سنُري القارىء كيف أن طرق ونتائج هذا البند يمكن استخدامها لإثبات حقائق غير تافهة في الزمر. عندما ننشىء الزمرة G/N حيث N ناظمية في G وإذا حدث وأن عرفنا بنْيَة G/N فإننـا نعلم بِنْيَة G «بالنسبة إلى N». صحيح، أننا نفقد بعض المعلومات المتعلقة بـ G ، ولكن غالبا ما تبقى معلومات كافية عن G/N يمكن عن طريقها استنتاج بعض المعلومات عن G . عندما نصور منظرًا معيّنا فإننا نحوّل الشيء ذا الأبعاد الثلاثة إلى تمثيل في بعدين. وفضلا عن ذلك، فإننا نستطيع من النظر إلى الصورة أن نعرف معلومات كثيرة عن المنظر المصور.

إن البرهان المقدم في التطبيقين الآتيين على بعض الأفكار المطوّرة حتى الآن، ليس أفضل ما يمكن . إذ سنثبت النتيجتين لاحقاً في وضع أكثر شمولية وبطريقة أسهل. ولكننا نستخدم هذا العرض هنا لأنه يوضح لنا بشكل جيد بعض المفاهيم في نظرية الزمر.

تطبيق (١) : (مبرهنة كوشي [Cauchy] للزمر الإبدالية)

لنفرض أن G زمرة إبدالية منتهية وأن $p|o(G)$ حيث p عدد أولي. **عندئذ يوجد عنصر $a\in G$ و$a\neq e$ بحيث يكون $a^p=e$.**

البرهان

سنبرهن على هذا التطبيق باستخدام الاستقراء الرياضي على رتبة G . بعبارة أخرى، سنفرض صحة المبرهنة لجميع الزمر الإبدالية التي رتبها تقل عن رتبة G . واستنادا إلى ذلك سنثبت أن النتيجة محققة بالنسبة لـ G . ونبدأ الاستقراء بملاحظة أن المبرهنة صحيحة في حالة الزمر التي تحتوي على عنصر واحد.

إذا كانت G لا تحتوي على زمرة جزئية $H\neq(e)$ و$H\neq G$ فإنه وفقا لنتيجة سابقة في هذا الفصل يجب أن تكون G دائرية رتبتها عدد أولي. هذا العدد الأولي هو p . وفي

هذه الحالة تحتوي G على عناصر غير تافهة عددها $p-1$ ورتبة كل عنصر من هذه العناصر هي p .

لنفرض الآن أن G تحتوي على زمرة جزئية N بحيث تكون $G \neq N \neq (e)$.

إذا كان $p|o(N)$ فإنه وفقا لفرضية الاستقراء الرياضي يوجد عنصر $e \neq b \in N$ بحيث يكون $b^p=e$ وذلك لأن $o(N)<o(G)$ كما أن N إبدالية. وحيث إن $b \in N \subset G$ لذلك فإننا قد حصلنا على عنصر يحقق شرط المبرهنة.

لذلك نفرض الآن أن $p \nmid o(N)$. لما كانت G إبدالية وN ناظمية في G لذلك فإن G/N زمرة، كما أن $o(G/N) = \frac{o(G)}{o(N)}$ وبما أن $p \nmid o(N)$ لذا فإن

$$p \mid \frac{o(G)}{o(N)} < o(G)$$

أيضا فإن G/N إبدالية نظرا لأن G كذلك. ووفقا لفرضية الاستقراء الرياضي يوجد عنصر $X \in G/N$ يحقق العلاقة $X^p=e_1$ حيث e_1 هو العنصر المحايد في G/N . كما أن $X \neq e_1$.

ولكن صيغة العنصر X في G/N هي $X=Nb$ ، $b \in G$ وبناءً عليه نجد $X^p=(Nb)^p=Nb^p$ وحيث إن $e_1=Ne$ و $X^p=e_1$ و $X \neq e_1$ لذا نجد أن $Nb \neq N$ كما أن $Nb^p=N$ مما يعني أن $b^p \in N$ ، $b \notin N$.

واستنادا إلى إحدى نتائج مبرهنة لاجرانج، نجد أن $(b^p)^{o(N)}=e$ ، أي أن $b^{o(N)p}=e$.

ليكن $c=b^{o(N)}$ ، عندئذ $c^p=e$ ولكي نثبت أن العنصر c يحقق شرط المبرهنة يجب علينا أن نثبت أن $c \neq e$. فلنفرض أن $c=e$ عندئذ $b^{o(N)}=e$ ومن ثم فإن $(Nb)^{o(N)}=N$ وبالجمع ما بين $(Nb)^p=N$ وكون $p \nmid o(N)$ حيث p عدد أولي نحصل على $Nb=N$ وذلك يقتضي أن $b \in N$. وهذا تناقض. ومن ثم فإن $c \neq e$ كما أن $c^p=e$ وبهذا نكون قد انهينا الاستقراء وبه يتم البرهان.

تطبيق (٢) : (مبرهنة سيلو [Sylow] للزمر الإبدالية)

إذا كانت G زمرة إبدالية رتبتها $o(G)$ وكان p عددا أوليا بحيث ان $p^\alpha | o(G)$ و $p^{\alpha+1} \nmid o(G)$ فإن G تحتوي على زمرة جزئية رتبتها p^α .

البرهان

إذا كان $\alpha = 0$ فإن الزمرة الجزئية (e) تحقق استنتاج المبرهنة. لذلك نفرض أن $\alpha \neq o$ ، عندئذ $p|o(G)$ ووفقا للتطبيق الأول يوجد عنصر $e \neq a \in G$ بحيث يكون $a^p=e$. لنفرض أن $S=\{x \in G | x^{p^n}=e$ ، حيث n عدد صحيح ما$\}$. بما أن $a \in S$ و $a \neq e$ لذلك تكون $S \neq (e)$. إننا ندعي أن S زمرة جزئية من G . لما كانت S منتهية لذا فإنه يكفي أن نتحقق من أن S مغلقة. إذا كان $x;y \in S$ فإن $x^{p^n}=e$ و $y^{p^m}=e$ وبالتالي فإن $(xy)^{p^{n+m}} = x^{p^{n+m}} y^{p^{n+m}}=e$ [لقد استفدنا هنا من كون G إبدالية] وهذا يثبت أن $xy \in S$. بعد هذا ندعي أن $o(S)=p^\beta$ حيث $0<\beta \leq \alpha$. لبرهان ذلك، إذا كان q عددا أوليا معينا وكان $q|o(S)$ ، $q \neq p$. فإنه وفقا للتطبيق الأول، يوجد عنصر $e \neq c \in S$ بحيث يكون $c^q=e$ ، ومع ذلك فإن $c^{p^n}=e$ حيث n عدد صحيح معين لأن $c \in S$. ولما كان q,p^n أوليين نسبيا فبإمكاننا إيجاد عددين صحيحين λ و μ بحيث يكون $\lambda q+\mu p^n=1$ وبناء عليه فإن

$$c=c^1=c^{\lambda q+\mu p^n}=(c^{q^\lambda}(c^{p^n})^\mu)=e$$

ولكن ذلك يناقض كون $c \neq e$.

واستنادا إلى مبرهنة لاجرانج فإن $o(S)|o(G)$ ، لذلك فإن $\beta \leq \alpha$. لنفرض الآن أن $\beta<\alpha$ ولنعتبر الزمرة الإبدالية G/S . لما كان $\beta<\alpha$ وكانت $o(G/S)=\frac{o(G)}{o(S)}$ وكان أيضا $p|o(G/S)$ ، فإنه يوجد عنصر Sx $(x \in G)$ في G/S يحقق الشرط $Sx \neq S$ و $(Sx)^{p^n}=S$ حيث n عدد صحيح أكبر من الصفر.
لكن $S=(Sx)^{p^n}=Sx^{p^n}$ وهكذا فإن $x^{p^n} \in S$ وبالتالي $e=(x^{p^n})^{o(S)} = (x^{p^n})^{p^\beta} = x^{p^{n+\beta}}$.
ولذلك فإن x يحقق تماما المتطلبات اللازمة لكي ينتمي إلى S ، وبعبارة أخرى $x \in S$. ولذلك فإن $Sx=S$ مما يناقض كون $Sx \neq S$ وعليه فإن كون $\beta<\alpha$ غير ممكن وبالتالي فإن $\beta=\alpha$. وبناءً على ذلك فإن S هي الزمرة الجزئية المطلوبة ذات الرتبة p^α .

لنضفي على هذا التطبيق قوة أكثر وذلك بفرض أن T هي زمرة جزئية أخرى من G رتبتها p^α ، $T \neq S$ وعندئذ فإن $ST=TS$ لأن G إبدالية ولهذا فإن ST زمرة جزئية من G .

استنادا إلى مبرهنة (٢-٥-١) نجد

$$o(ST)=\frac{o(S)\,o(T)}{o(S\cap T)}=\frac{p^{\alpha}p^{\alpha}}{o(S\cap T)}$$

وحيث إن $S\neq T$ ، لذلك فإن $o(S\cap T) < p^{\alpha}$ وبالتالي فإن $o(ST) < p^{\gamma}$ حيث $\gamma>\alpha$. وبما أن ST زمرة جزئية من G فإن هذا يقتضي أن يكون $o(ST)|o(G)$ ، أي أن $p^{\gamma}|o(G)$ مما يناقض حقيقة أن α هو أكبر قوة للعدد p التي من أجلها $p^{\alpha}|o(G)$ وبناءً عليه فإنه لا يوجد مثل هذه الزمرة الجزئية (أي T)، أي أن S هي الزمرة الجزئية الوحيدة ذات الرتبة p^{α} وبهذا نكون قد برهنا النتيجة الآتية.

نتيجة

إذا كانت G إبدالية رتبتها $o(G)$ وكان $p^{\alpha}|o(G)$ و $p^{\alpha+1}\nmid o(G)$ فإنه يوجد زمرة جزئية وحيدة في G رتبتها p^{α} .

إذا نظرنا إلى الزمرة $G=S_3$ التي ليست إبدالية حيث $o(G)=2.3$ فإننا نجد أن G تحتوي على ثلاث زمر جزئية مختلفة رتبة كل منها تساوي 2 وهي على الترتيب $\{e,\phi\}$ و $\{e,\phi\psi\}$ و $\{e,\phi\psi^2\}$ وبالتالي فإن النتيجة تؤكد أن الوحدانية ليست محققة في حالة الزمر غير الإبدالية بيد أن مبرهنة سيلو سارية المفعول لجميع الزمر المنتهية.

نعود الآن إلى موضوع التشاكل. لنفرض أن ϕ تشاكل من G على $\bar{G}$ نواته هي K وأن $\bar{H}$ زمرة جزئية من $\bar{G}$ ولتكن $H=\{x\in G|\phi(x)\in\bar{H}\}$. إننا ندَّعي أن H زمرة جزئية من G تحتوي K . إن كون $H\supset K$ واضح ذلك لأنه إذا كان $x\in K$ فإن $\phi(x)=\bar{e}\in\bar{H}$ ومن ثم فإن $H\supset K$. لنفرض الآن أن $x,y\in H$ عندئذ $\phi(x)\in\bar{H}$ و $\phi(y)\in\bar{H}$ وهكذا فإن $\phi(xy)=\phi(x)\,\phi(y)\in\bar{H}$ وبناءً عليه، $xy\in H$ مما يعني أن H مغلقة بالنسبة لحاصل الضرب في G . وفضلا عن ذلك، إذا كان

$x\in H$ فإن $\phi(x)\in\bar{H}$ وبالتالي $\phi(x^{-1})=\phi(x)^{-1}\in\bar{H}$ مما يترتب عليه أن يكون $x^{-1}\in H$. وهكذا فإننا قد برهنا على إدعائنا بأن H زمرة جزئية من G . بالإضافة إلى ذلك ماذا يمكن القول عن الحالة التي تكون فيها $\bar{H}$ ناظمية في $\bar{G}$ ؟ لنفرض أن $g\in G$ و$h\in H$ عندئذ $\phi(h)\in\bar{H}$ ومن ثم فإن $\phi(ghg^{-1})=\phi(g)\phi(h)\phi(g)^{-1}\in\bar{H}$ لأن $\bar{H}$ ناظمية في $\bar{G}$. وبالتالي فإن $ghg^{-1}\in H$ أي أن H ناظمية في G .

أمر آخر جدير بالملاحظة هو أن التشاكل ϕ من G على $\bar{G}$ عندما يعمل على عناصر H فقط، فإنه يحدث تشاكلا من H على $\bar{H}$ نواته هي K نفسها. ولما كانت $H\supset K$ فإنه وفقًا لمبرهنة (٢-٧-١) نجد أن $\bar{H}\approx H/K$.

وعلى العكس، لنفرض أن L زمرة جزئية من G وأن $K\subset L$ ولتكن $\bar{L}=\{\bar{x}\in\bar{G}|\bar{x}=\phi(l), l\in L\}$ عندئذ يستطيع القارىء أن يتحقق من أن $\bar{L}$ زمرة جزئية من $\bar{G}$. هل يمكن وصف الزمرة الجزئية $T=\{y\in G|\phi(y)\in\bar{L}\}$ بوضوح؟ واضح أن $L\subset T$. هل يوجد أي عنصر $t\in T$ بحيث يكون $t\notin L$ ؟ لنفرض أن $t\in T$ عندئذ $\phi(t)\in\bar{L}$ ومن تعريف $\bar{L}$ نجد $\phi(t)=\phi(l)$ حيث $l\in L$. وبناءً عليه فإن $\phi(tl^{-1})=\phi(t)\,\phi(l)^{-1}=\bar{e}$ وبالتالي $tl^{-1}\in K\subset L$ أي أن t ينتمي إلى Ll التي تساوي L . وبعبارة أخرى، لقد برهنا على أن $T\subset L$ وهذه النتيجة مع كون $L\subset T$ تقتضي أن $L=T$. بهذا نكون قد أنشأنا تقابلا بين مجموعة الزمر الجزئية في $\bar{G}$ ومجموعة الزمر الجزئية من G التي تحتوى K . وبالإضافة إلى ذلك نجد وفقا لهذا التقابل أن كل زمرة جزئية ناظمية في G تقابل زمرة جزئية ناظمية في $\bar{G}$.

ونلخص هذه الفقرات في التمهيدية الآتية .

تمهيدية (٢-٧-٥)

ليكن ϕ تشاكلا من G على $\bar{G}$ نواته هي K ولنعرف H كما يلي $H=\{x\in G|\phi(x)\in\bar{H}\}$ حيث $\bar{H}$ زمرة جزئية من $\bar{G}$. عندئذ تكون H زمرة جزئية من G تحتوي K . وإذا كانت

$\bar{H}$ ناظمية في $\bar{G}$ فإن H ناظمية في G وبالإضافة إلى ذلك فإنه ينشأ عن هذا الترابط تقابل من مجموعة كل الزمر الجزئية من $\bar{G}$ على مجموعة كل الزمر الجزئية من G التي تحتوي K .

نود الآن إثبات مبرهنة عامة حول العلاقة بين زمرتين متشاكلتين.

مبرهنة (٢ـ٧ـ٢)

ليكن ϕ تشاكلا من G على $\bar{G}$ نواته K . ولتكن $\bar{N}$ زمرة جزئية ناظمية من $\bar{G}$ و $N=\{x\in G|\phi(x)\in\bar{N}\}$ عندئذ $G/N \approx \bar{G}/\bar{N}$ وبعبارة أخرى $G/N\approx(G/K)/(N/K)$.

البرهان

كما نعلم، يوجد تشاكل θ من $\bar{G}$ على $\bar{G}/\bar{N}$ معرف كما يلي $\theta(\bar{g})=\bar{N}\bar{g}$.
الآن نعرف التطبيق $\psi:G\to\bar{G}/\bar{N}$ كما يلي $\psi(g)=\bar{N}\phi(g)$ حيث $g\in G$. إن ψ غامر، لأنه إذا كان $\bar{g}\in\bar{G}$ فإن $\bar{g}=\phi(g)$ حيث $g\in G$ ونظرا لأن ϕ غامر لذلك فإنه يمكن كتابة العنصر $\bar{N}\bar{g}$ في $\bar{G}/\bar{N}$ على الصيغة $\psi(g)=\bar{N}\phi(g)$ إذا كان $a,b\in G$ فإنه ـ وفق تعريف التطبيق ψ ـ يكون $\psi(ab)=\bar{N}\phi(ab)$ ولكن $\phi(ab)=\phi(a)\phi(b)$ لأن ϕ تشاكل وبالتالي:

$$\bar{N}\,\phi(a)\,\phi(b)=\bar{N}\,\phi(a)\,\bar{N}\,\phi(b)=\psi(a)\,\psi(b).$$

وهكذا فإن ψ تشاكل من G على $\bar{G}/\bar{N}$. ما هي نواة ψ ؟ لنفرض أن T هي نواة ψ . أولا، إذا كان $n\in N$ فإن $\phi(n)\in\bar{N}$ وبالتالي $\psi(n)=\bar{N}\phi(n)=\bar{N}$ حيث $\bar{N}$ هو العنصر المحايد في $\bar{G}/\bar{N}$ وهذا يثبت أن $N\subset T$.
ومن ناحية أخرى، إذا كان $t\in T$ فإن $\psi(t)$ هو العنصر المحايد في $\bar{G}/\bar{N}$ الذي يساوي $\bar{N}$ ، ولكن $\psi(t)=\bar{N}\phi(t)$ وبالتالي فإن: $\bar{N}=\bar{N}\phi(t)$ وهذا يعني أن $\phi(t)\in\bar{N}$. ومن تعريف N نجد أن $t\in N$ ، أي أن $T\subset N$ وبهذا نكون قد برهنا على أن نواة ψ هي N . وعندئذ يكون ψ تشاكلا من G على $\bar{G}/\bar{N}$ نواته هي N .

واستنادا إلى المبرهنة (٢ـ٧ـ١) نستنتج أن $G/N\approx\bar{G}/\bar{N}$ وهذا يثبت القسم الأول من المبرهنة. إن القسم الثاني من المبرهنة ينتج من ملاحظة أن $\bar{G}\approx G/K$ ، $\bar{N}\approx N/K$ ومنه نجد $\bar{G}/\bar{N}\approx(G/K)/(N/K)$. (وهذا ينتج أيضا كنتيجة لمبرهنة ٢ـ٧ـ١).

مسائل

١ ـ تحقق مِمَّا إذا كانت التطبيقات الآتية هي تشاكلات ثم أوجد نواة التشاكل.

(ا) G هي زمرة الأعداد الحقيقية غير الصفرية بالنسبة لعملية الضرب و $\bar{G} = G$ و $\phi(x)=x^2$ لكل $x \in G$.

(ب) G و $\bar{G}$ كما في (ا) و $\phi(x)=2^x$.

(جـ) G هي زمرة الأعداد الحقيقية بالنسبة لعملية الجمع و $\bar{G} = G$ و $\phi(x)=x+1$ لكل $x \in G$.

(د) G و $\bar{G}$ كما في (جـ) و $\phi(x)=13x$ ، $x \in G$.

(هـ) G أية زمرة إبدالية و $\bar{G} = G$ و $\phi(x)=x^5$ لكل $x \in G$.

٢ ـ لنفرض أن G أية زمرة وأن $g \in G$ عنصر معين ولنعرف $\phi: G \to G$ بالعلاقة $\phi(x)=gxg^{-1}$. أثبت أن ϕ تماثل من G إلى G.

٣ ـ لنفرض أن G زمرة إبدالية منتهية رتبتها $o(G)$ وأن n عدد صحيح بحيث يكون $(n,o(G)) = 1$. برهن على أن كل عنصر $g \in G$ يمكن كتابته على الصيغة $g=x^n$ حيث $x \in G$.

إرشاد: اعتبر التطبيق $\phi: G \to G$ المعرف كما يلي $\phi(g) = g^n$ ، ثم برهن على أنه تماثل من G على نفسها.

٤ ـ (ا) إذا كانت G أية زمرة وU مجموعة جزئية منها. ولتكن $\hat{U}$. أصغر زمرة جزئية من G تحوى U . أثبت وجود مثل هذه الزمرة الجزئية $\hat{U}$ في G.

[**يطلق على $\hat{U}$. الزمرة الجزئية المولدة بالمجموعة U**].

(ب) إذا كان $gug^{-1} \in U$ لكل $g \in G$ ولكل $u \in U$. فأثبت أن $\hat{U}$. زمرة جزئية ناظمية في G.

٥ ـ لتكن $U=\{xyx^{-1}y^{-1} | x,y \in G\}$. يرمز لـ $\hat{U}$. في هذه الحالة بالرمز G' **ويطلق عليها زمرة المبدلات الجزئية في G**

(ا) برهن على أن G' زمرة جزئية ناظمية في G.

(ب) برهن على أن G/G' إبدالية.

(جـ) إذا كانت G/N إبدالية فأثبت أن $N \supset G'$.

(د) إذا كانت H زمرة جزئية من G و $H \supset G'$ فإن H زمرة جزئية ناظمية في G .

٦ - إذا كانت N,M زمرتين جزيئيتين ناظميتين من G
فأثبت أن $NM/M \approx N/N \cap M$.

٧ - لتكن V هي مجموعة الأعداد الحقيقية ولنعرف التطبيق $\tau_{ab}:V \to V$ ، حيث $a,b \in V$ بالعلاقة $\tau_{ab}(x)=ax+b$ ولتكن$G=\{\tau_{ab}|a,b \in V, a \neq O\}$ و $N=\{\tau_{1b} \in G\}$.
أثبت أن N زمرة جزئية ناظمية في G وأن G/N تماثل زمرة الأعداد الحقيقية غير الصفرية بالنسبة لعملية الضرب .

٨ - لتكن G هي الزمرة الزوجية والمعرفة على أنها مجموعة كل الرموز $x^i y^j$ ، $i=0,1$ و $j=1,2,...n-1$ ، حيث $x^2=e$ و $y^n=e$ و $xy=y^{-1}x$.
أثبت ما يلي :
(ا) إن الزمرة الجزئية $N=\{e,y,...y^{n-1}\}$ هي زمرة جزئية ناظمية في G .
(ب) $G/N \approx W$ حيث $W=\{1,-1\}$ هي زمرة بالنسبة لعملية ضرب الأعداد الحقيقية .

٩ - برهن على أن مركز الزمرة هو دوما زمرة جزئية ناظمية .

١٠ - برهن على أن الزمرة التي رتبتها 9 هي زمرة إبدالية .

١١ - إذا كانت G زمرة غير إبدالية وكانت $o(G)=6$
فأثبت أن $G \approx S_3$.

١٢ - إذا كانت G زمرة إبدالية وكانت N زمرة جزئية من G
فأثبت أن G/N إبدالية .

١٣ - أوجد مركز الزمرة الزوجية الواردة في المسألة (٨) .

١٤ - أوجد زمرة المبدلات الجزئية ، أي G' للزمرة الزوجية الواردة في المسألة (١٣) .

١٥ - لتكن G هي زمرة الأعداد المركبة غير الصفرية بالنسبة لعملية الضرب، ولتكن N هي مجموعة الأعداد المركبة التي قيمتها المطلقة تساوي الواحد (أي أن $a+ib \in N$ إذا كان $a^2+b^2=1$) . أثبت أن G/N تماثل زمرة الأعداد الحقيقية الموجبة بالنسبة لعملية الضرب .

١٦ - لتكن G هي زمرة الأعداد المركبة غير الصفرية بالنسبة لعملية الضرب وأن $\bar{G}$ هي زمرة المصفوفات $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ من النوع 2×2 حيث b,a عددان حقيقيان لا يساويان الصفر معا وذلك بالنسبة لعملية ضرب المصفوفات. أثبت أن G تماثل $\bar{G}$ وذلك بإيجاد تماثل من G على $\bar{G}$.

١١* - لتكن G هي زمرة الأعداد الحقيقية بالنسبة لعملية الجمع و N هي الزمرة الجزئية المكونة من الأعداد الصحيحة. أثبت أن G/N متماثلة مع زمرة الأعداد المركبة التي قيمتها المطلقة تساوي الواحد وذلك بالنسبة لعملية الضرب.

١٨ - لتكن G هي زمرة المصفوفات الحقيقية $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ من النوع 2x2 حيث $ad-bc\neq o$ وذلك بالنسبة لعملية ضرب المصفوفات: ولتكن

$$N = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1\}$$

أثبت أن $N\supset G'$ حيث G' هي زمرة المبدلات الجزئية في G.

١٩* في المسألة (١٨)، أثبت أنه في الحقيقة أن $G'=N$.

٢٠ - لتكن G هي زمرة المصفوفات الحقيقية $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ من النوع 2x2 حيث $ad\neq o$ وذلك بالنسبة لعملية ضرب المصفوفات.

أثبت أن G' هي تماما مجموعة المصفوفات من الصيغة $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.

٢١ - لتكن S_1 و S_2 مجموعتين، ولنفرض أنه يوجد تقابل ψ من S_1 إلى S_2.

أثبت وجود تماثل من $A(S_1)$ إلى $A(S_2)$ حيث $A(S)$ هي مجموعة كل التقابلات من S على نفسها.

(٢ - ٨) التماثلات الذاتية

لقد عرفنا ودرسنا، في البند السابق، مفهوم التشاكل من زمرة إلى أخرى. حالة خاصة من ذلك ولكنها ذات أهمية هي عندما يكون التشاكل من الزمرة على نفسها. هنا نستخدم كلمة «على» عَمدا، ذلك أنه توجد زمر وتشاكلات تطبق هذه الزمر إلى - وليس على - نفسها. وأبسط مثال على ذلك هو أنه إذا كانت G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع وكان $\phi:G\to G$ وفق القاعدة $\phi(x)=2x$ لكل $x\in G$. وحيث

إن $\phi:x+y \rightarrow 2(x+y) = 2x+2y$ لذلــك فإن ϕ تشــاكـل . أيضـا إذا كانت صورتـا x ، y ـ وفق التـطبيق ϕ ـ متسـاويتـين فإن $2x=2y$ يقتضي أن $x=y$ أي أن ϕ تماثل، بيد أن ϕ ليس غامرا، ذلك أن صورة أي عدد صحيح وفق التطبيق ϕ هو عدد صحيح زوجي، وعلى سبيل المثال فإن العـدد 1 ليس صورة لأي عنصر من G تحت تأثير ϕ . إن اهتمامنا سيكون منصبا على دراسة التماثل من زمرة على نفسها.

تعريف

التماثل الذاتي (automorphism) لزمرة ما G هو التماثل من G على نفسها.

وكما ذكرنا في الفصل الأول فإنه عندما نتحدث عن التطبيقات من مجموعة إلى نفسهـا، فإننـا سنكتب التـطبيقـات من اليمين، وهكذا إذا كان $T:S \rightarrow S$ و$x \in S$ فإن xT هي صورة العنصر x تحت تأثير T .

ليكن I هو التـطبيق على G الـذي يرسـل كل عنصر إلى نفسـه، أي أن، $xI=x$ لكل $x \in G$. إن I تماثل ذاتي على G كما يبدو ذلك واضحا.

لتكن $\mathscr{A}(G)$ ترمـز إلى مجمـوعـة كل التـماثـلات الذاتية على الزمرة G . إن $\mathscr{A}(G)$ مجمـوعـة جزئية من $A(G)$ التي هي مجموعة التطبيقات الأحادية من G على نفسهـا، لذلـك يمكن استخـدام الضرب المعـرف على $A(G)$ من أجـل $\mathscr{A}(G)$ ـ أي تركيب التـطبيقـات ـ ولما كان هذا الضرب محققا لقانون التجميع في $A(G)$ ، فإنـه من باب أولى محقق في $\mathscr{A}(G)$ ، أيضـا فإن عنصر الوحدة I في $A(G)$ موجودة في $\mathscr{A}(G)$ ، لذلك فإن $\mathscr{A}(G)$ ليست خالية.

إن الحقيقـة التي تجب علينـا محاولـة إثبـاتهـا هي أن $\mathscr{A}(G)$ زمـرة جزئية من $A(G)$ وبالتالي فإن $\mathscr{A}(G)$ زمرة بكل ما في الكلمة من معنى.

إذا كان $T_1, T_2 \in \mathscr{A}(G)$ ، فإننا نعلم أن $T_1, T_2 \in A(G)$ ، بيد أننا نريد أن يكون هذا العنصر في المجموعة الصغرى $\mathscr{A}(G)$ وللتحقق من ذلك نجد أنه لكل $x, y \in G$ يكون

$$(xy)\,T_1 = (x\,T_1)\,(y\,T_1)\,,$$
$$(xy)\,T_2 = (x\,T_2)\,(y\,T_2)$$

ولهذا فإن

$$(xy)\,T_1T_2 = ((xy)T_1)T_2 = ((x\,T_1)(y\,T_1))\,T_2$$
$$= ((x\,T_1)T_2)\,((y\,T_1)\,T_2) = (x\,T_1T_2)\,(y\,T_1T_2)$$

مما يعني أن $T_1T_2 \in \mathscr{A}(G)$.

بقي حقيقة أخرى تحتاج إلى إيضاح لكي تكون $\mathscr{A}(G)$ زمرة جزئية من $A(G)$ تلك هي أنه إذا كان $T \in \mathscr{A}(G)$ فإن $T^{-1} \in \mathscr{A}(G)$.

إذا كان x ، $y \in G$ فإن :

$$[(xT^{-1})\,(yT^{-1})]\,T = [(xT^{-1})T]\,[(yT^{-1})T]$$
$$= (xI)\,(yI) = xy$$

وهكذا فإن $(xy)T^{-1} = ((xT)^{-1})(yT^{-1})$ ويقتضي هذا أن $T^{-1} \in \mathscr{A}(G)$.

بهذه الملاحظات نكون قد أثبتنا التمهيدية الآتية .

تمهيدية (٢-٨-١)

إذا كانت G زمرة فإن مجموعة التماثلات الذاتية $\mathscr{A}(G)$ للزمرة G هي زمرة أيضا .

طبعا ، حتى الآن ، لا نعلم طريقة ، في الحالة العامة ، لمعرفة ما إذا كانت $\mathscr{A}(G)$ تحتوي على عناصر غير I .

فإذا كانت G زمـرة تحتـوي على عنصرين فقط فإن باستطاعة القارىء إثبات أن $\mathscr{A}(G)$ تحتـوي على I فقط. وفي حالـة الزمر التي تحتوي على أكثر من عنصرين فإن $\mathscr{A}(G)$ تحتوي دائما على أكثر من عنصر.

إن ما نريده هو عينـة من التـماثلات الذاتية أغنى في خواصها من تلك التي لدينـا (أي، I). فإذا كانت G إبـدالية وكان يوجد عنصر $x_0 \in G$ بحيث $x_0 \neq x_0^{-1}$ ، فإننـا نستطيع كتابة تماثل ذاتي صريح، هو التطبيق T المعرف بالعلاقة $xT=x^{-1}$ لكل $x \in G$. إن T غامر لأية زمرة G . ولكل زمرة إبدالية G يكون لدينا.

$$(xy)\,T = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = (xT)(yT)$$

أيضا فإن $x_0T=x_0^{-1} \neq x_0$ ، لهذا فإن $T \neq I$.

ورغم ذلك فإن صنف الزمر الإبدالية محدود قليلا ولهذا فإننا نود أن يكون لدينا تماثـلات ذاتية لزمر غير إبدالية. والغريب حقا هو أن مهمة الحصول على التماثلات الذاتية لمثل هذه الزمر أسهل منها في حالة الزمر الإبدالية.

لتكن G زمـرة ولنفـرض أن $g \in G$ ، عنـدئذ نعرف التطبيق $T_g:G \rightarrow G$ كما يلي $x\,T_g = g^{-1}xg$ لكـل $x \in G$. إننا ندعي أن T_g تماثل ذاتي على G . أولا، إن T غامر لأنه إذا كان $y \in G$ وفرضنا أن $x=gyg^{-1}$ فإن

$$xT_g = g^{-1}(x)g = g^{-1}(gyg^{-1})\,g = y$$

لذا فإن T_g غامر.

لنفرض الآن أن $x,y \in G$ ، عندئذ

$$(xy)T_g = g^{-1}(xy)g = g^{-1}(xgg^{-1}y)g = (g^{-1}xg)(g^{-1}yg) = (xT_g)(yT_g)$$

أي أن T_g تشاكل من G على نفسها.

وفضلا عن ذلك، فإن T_g أحادي، لأنه إذا كان $xT_g=yT_g$ فإن $g^{-1}xg=g^{-1}yg$ ، واستنـادا إلى قوانـين الاختـزال نجد أن $x=y$. إن T_g يدعى **التماثل الذاتي الداخلي**

(Inner automorphism) المقــابــل للعنصر g . فإذا كانت G ليست إبــدالية فإنـه يوجــد عنصران $a,b\in G$ بحــيث يكــون $ab\neq ba$ وعــنــدئــذ $bT_a=a^{-1}ba\neq b$ ولذلك فإن $T_a\neq I$. وهكذا فإنه يوجد تماثلات ذاتية غير تافهة للزمر غير الإبدالية .

لتكن $\mathscr{I}(G) = \{T_g\in \mathscr{A}(G)|g\in G\}$. إن حساب T_{gh} حيث $h\in G$ ، g قد يكون مهما إلى حد ما، لذلك نفرض أن $x\in G$ ومن تعريف T_g .

$xT_{gh}=(gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = (g^{-1}xg)\, T_h = (xT_g)\, T_h = xT_gT_h$

وبالتالي فإن $T_{gh} = T_gT_h$.

إن هذه الملاحظة مهمة وموحية في الوقت نفسه . إنها مهمة لأنه ينتج عنها مباشرة أن $\mathscr{I}(G)$ زمرة جزئية من $\mathscr{A}(G)$ (تحقق من ذلك). إن $\mathscr{I}(G)$ غالبا ما تدعى **بزمرة التماثلات الذاتية الداخلية** للزمرة G . كما أنها موحية، لأنه إذا إعتبرنا التطبيق $\psi:G\to\mathscr{A}(G)$ المعرف بالعلاقة $\psi(g)=T_g$ لكل $g\in G$ فإن $\psi(gh) = T_{gh} = T_gT_h = \psi(g)\psi(h)$ أي أن ψ تشاكل من G إلى $\mathscr{A}(G)$ والتي صورته هي $\mathscr{I}(G)$. ما هي نواة ψ ؟ لنفرض أنها K وأن $g_0\in K$ ، عندئذ $\psi(g_0)=I$ ، وبعبارة أخرى، $T_{g_0}=I$ ولكن هذا يعني أنه لأي $x\in G$ يكون $xT_{g_0}=x$. ومع ذلك، فإن $xT_{g_0}=g_0^{-1}xg_0$ وبالتالي فإن $x=g_0^{-1}xg_0$ لكل $x\in G$ وهكذا فإن $g_0x= g_0g_0^{-1}\, xg_0 = xg_0$ مما يعني أن g_0 تتبادل مع جميع عناصر G ، ولكننا عَرَّفنا مركز الزمرة G ، أي Z ، بأنه تماما كل العناصر في G التي تتبادل مع كل عنصر في G (انظر تمرين ١٥ بند ٢ـ٥). وهكذا فإن $K\subset Z$.

كذلــك إذا كان $x\in Z$ فإن $xT_z=z^{-1}xz=x$ (وذلــك لأن $zx=xz$) . أي أن $T_z=I$ وبـالتـالي فإن $z\in K$ وهـذا يقتضي أن $Z\subset K$. لقـد أثبتنـا أن $K\subset Z$ و $Z\subset K$ ، لذلك نجد أن $K=Z$.

ويمكن تلخيص ما سبق بقـولنـا إن ψ تشاكل من G إلى $\mathscr{A}(G)$ صورته هي $\mathscr{I}(G)$ ونــواتــه هي Z . واســتــنــادا إلى مبرهــنــة (٢ـ٧ـ١) فإن $\mathscr{I}(G) \approx G/Z$. وللتأكيد على هذه النتيجة العامة فإننا ندونها على هيئة تمهيدية .

تمهيدية (٢-٨-٢)

$\mathcal{A}(G) \approx G/Z$ حيث $\mathcal{A}(G)$ هي زمرة التماثلات الذاتية الداخلية للزمرة Z,G هو مركز الزمرة G .

لنفرض الآن أن ϕ تماثل ذاتي على الزمرة G وأن $a \in G$ وأن رتبة a هي n (أي أن $a^n=e$ ، n هو أقل عدد صحيح موجب يحقق هذه العلاقة). عندئذ $\phi(a)^n=\phi(a^n)=\phi(e)=e$ ، أي أن $\phi(a)^n=e$. فإذا كان $\phi(a)^m=e$ حيث $0<m<n$ فإن $\phi(a)^m=\phi(a^m)=e$ مما يؤدي إلى أن $a^m=e$ لأن ϕ أحادي، وهذا تناقض. وبالتالي نحصل على التمهيدية الآتية:

تمهيدية (٢-٨-٣)

لتكن G زمرة و ϕ تماثلا ذاتيا على G فإذا كان a عنصرا من G رتبته هي $o(a)>0$ فإن $o(\phi(a))=o(a)$

يمكن استخدام التماثلات لبناء زمر جديدة من زمر معروفة ولكن قبل أن نوضح هذا تجريديا نعتبر المثال الخاص الآتي:

لتكن G هي الزمرة الدورية التي رتبتها 7 ، أي أن G تتكون من العناصر a^i حيث $a^7=e$. إن التطبيق $\phi:a^i \to a^{2i}$ هو تماثل ذاتي رتبته تساوي 3 أي أن $\phi^3=1$ ويمكن التأكد من ذلك بسهولة. لنفرض أن x هو رمز يخضع للشروط الآتية: $x^{-1}a^ix=\phi(a^i)=a^{2i}$ و $x^3=e$ ولنعتبر كل الرموز من الصيغة x^ia^j حيث $i=0,1,2$ و $j=0,1,2,\ldots,6$.

ونؤكد هنا على أن $x^ia^j=x^ka^l$ إذا وفقط إذا كان $i=k \bmod 3$ و $j=l \bmod 7$. إننا نضرب هذه الرموز ببعضها مستخدمين القواعد الآتية: $x^3=a^7=e, x^{-1}ax=a^2$ فمثلا ،

$$(xa)(xa^2)=x(ax)a^2=x(xa^2)a^2=x^2a^4$$

ويمكن للقارىء التحقق بأنه يمكن الحصول بهذه الطريقة على زمرة غير إبدالية رتبتها تساوي 21.

وعلى العموم، إذا كانت G زمرة وكان T تماثلا ذاتيا غير داخلي رتبته تساوي r ثم اخترنا رمزا هو x واعتبرنا كل العناصر x^ig حيث $i=0,\pm1,\pm2,...$ ، $g\in G$ التي تخضع للشرط وهو أن $x^ig=x^{i'}g'$ إذا وفقط إذا كان $i\equiv i' \bmod r$ و $g=g'$ و $x^{-1}g^ix=gT^i$ لجميع قيم i فإننا، بهذه الطريقة نحصل على زمرة أكبر هي {G,T} كما أن G ناظمية في {G,T} و {G,T}/G تماثل الزمرة المولدة بالعنصر T وهي الزمرة الدورية التي رتبتها تساوي r.

نختتم هذا البند بتعيين $\mathscr{A}(G)$ لجميع الزمر الدورية.

مثـــال (٢ـ٨ـ١)

لتكن G هي الزمرة الدورية المنتهية التي رتبتها تساوي r و $G=(a)$ ، $a^r=e$.

ولنفرض أن T تماثل ذاتي على G. وحيث إن $a^iT=(aT)^i$ لذا فإن معرفة aT تعين a^iT ، ووفْقــا لذلـك فإن gT قد تعـين وذلـك لكـل $g\in G=(a)$. وعليه فإننـا سنعتـبر فقط الصـور الممكنة للعنصر a تحت تأثير T. كذلك بما أن $aT\in G$ وبما أن كل عنصر من G هو إحـدى قوى a ، لذلـك فإن $aT=a^t$ حيث $0<t<r$. وبـما أن T تماثـل ذاتي، فإن رتبـة aT يجب أن تساوي رتبة a (تمهيدية ٢ـ٨ـ٣). إن هذا الشرط يفرض على t أن يكون أوليا بالنسبة إلى r ، لأنه إذا كان d|t و d|r فإن

$(aT)^{\frac{r}{d}}=a^{t(\frac{r}{d})}=a^{r(\frac{t}{d})}=e$ أي أن رتبة aT قاسمة للعدد $(\frac{r}{d})$

وبـالجمـع ما بين هذه الحقيقـة وتلك التي تنص على أن رتبـة aT هي r نستنتج أن $d=1$.

ومن ناحية أخرى، فإنه لأي عدد s أولي بالنسبة إلى r حيث $0<s<r$ ، يكون التـطبيق $S:a^i\to a^{si}$ تماثـلا ذاتيا على G. وهكـذا فإن $\mathscr{A}(G)$ تتقابل مع الزمرة U_r من الأعداد الصحيحة الأصغر من r والأولية بالنسبة إليه وذلك بالنسبة للضرب قياس r. إننا ندعي، ليس فقط، وجود تقابل بل إن هذا التقابل هو في الواقع تماثل. دعنا نرقم عناصر $\mathscr{A}(G)$ على الشكل T_i حيث $T_i:a\to a^i$ كما أن i أولي بالنسبة إلى r و $0<i<r$.

الآن $T_iT_j:a\to a^i\to(a^i)^j=a^{ij}$ ، أي أن $T_iT_j=T_{ij}$ إن التـطبيق $i\to T_i$ يظهـر لنـا التماثل من U_r على $\mathscr{A}(G)$. وعندئذ، نجد هنا أن $\mathscr{A}(G)\approx U_r$.

مثال (٢-٨-٢)

سنأخذ هنا G لتكون الزمرة الدورية غير المنتهية أي أن G تتكون من جميع العناصر a^i ، $i=0,\pm1,\ldots$ ، حيث نفرض هنا أن $a^i=e$ إذا وفقط إذا كان $i=0$. لنفرض أن T تماثل ذاتي على G. كما في المثال (٢-٨-١) $aT=a^t$.

السؤال الذي يطرح نفسه هو: ما هي قيم t الممكنة؟

لما كان T تماثلا ذاتيا على G لذلك فإنه يطبق G على نفسها ولهذا فإن $a=gT$ حيث $g\in G$.

وهكذا فإن $a=a^iT=(aT)^i$ ، حيث i عدد صحيح ولما كان $aT=a^t$ لذا فإنه يجب أن يكون لدينا $a=a^{ti}$ وبالتالي فإن $a^{ti-1}=e$ ومن ثم فإن $ti-1=0$ أي أن $ti=1$ وبما أن i ، t عددان صحيحان فإنه من الواضح $t=\pm1$.

وفي كلتا الحالتين ينشأ عن قيمتي t تماثلان ذاتيان، فعندما $t=1$ نحصل على التماثل الذاتي المحايد I. وعندما $t=-1$ نحصل على التماثل الذاتي $T:g\rightarrow g^{-1}$ لكل عنصر g من الزمرة الدورية G وهكذا فإن $\mathscr{A}(G)$ تماثل زمرة دورية رتبتها تساوي 2.

مسائل

١ - هل التطبيقات الآتية تماثلات ذاتية على الزمر المعرفة؟

(ا) G هي زمرة الأعداد الصحيحة بالنسبة لعملية الجمع و $T:x\rightarrow -x$.

(ب) G هي مجموعة الأعداد الحقيقية الموجبة بالنسبة لعملية الضرب، $T:x\rightarrow x^2$.

(جـ) G هي الزمرة الدورية التي رتبتها تساوي 12 ، $T:x\rightarrow x^3$.

(د) G هي الزمرة S_3 و $T:x\rightarrow x^{-1}$.

٢ - لتكن G زمرة و H زمرة جزئية منها و T تماثل ذاتي على G ولتكن $(H)T=\{hT|h\in H\}$. أثبت أن $(H)T$ زمرة جزئية من G.

٣ - لتكن G زمرة و T تماثل ذاتي على G و N زمرة جزئية ناظمية في G. أثبت أن $(N)T$ زمرة جزئية ناظمية في G.

٤ - إذا كانت $G=S_3$ فأثبت أن $G\approx\mathscr{I}(G)$.

٥ - أثبت أنه لأية زمرة G تكون $\mathscr{I}(G)$ زمرة جزئية ناظمية في $\mathscr{A}(G)$. [إن الزمرة $\mathscr{A}(G)/\mathscr{I}(G)$ تدعى **زمرة التماثلات الذاتية الخارجية على G**].

٦ - لتكن G هي الزمرة التي رتبتها تساوي 4 حيث

$$G=\{e,a,b,ab\}, \quad a^2=b^2=e, \quad ab=ba$$

عين $\mathscr{A}(G)$.

٧ - (ا) يقال عن الزمرة الجزئية C من G إنها **زمرة جزئية مميزة** (Characteristic subgroup) من G إذا كان $(C)T\subset C$ لكل تماثل ذاتي T على G. برهن على أن الزمرة الجزئية المميزة ناظمية في G.

(ب) أثبت أن عكس (ا) غير صحيح .

٨ - أثبت أن زمرة المبدلات الجزئية G' هي زمرة جزئية مميزة (انظر مسألة ٥ بند ٢-٧) .

٩ - إذا كانت G زمرة وكانت N زمرة جزئية ناظمية في G و M زمرة جزئية مميزة في N فأثبت أن M زمرة جزئية ناظمية في G.

١٠ - لتكن G زمرة منتهية و T تماثل ذاتي على G بحيث أن $xT=x$ إذا وفقط إذا كان $x=e$ حيث $x\in G$. أثبت أن كل عنصر $g\in G$ يمكن تمثيله على الصيغة $g=x^{-1}(xT)$ حيث $x\in G$.

١١ - لتكن G زمرة منتهية و T تماثل ذاتي على G بحيث أن $xT=x$ إذا وفقط إذا كان $x=e$ حيث $x\in G$ ولنفرض أيضا أن $T^2=I$. أثبت أن G يجب أن تكون إبدالية .

١٢* - لتكن G زمرة منتهية ولنفرض أن T تماثل ذاتي ينقل أكثر من ثلاثة أرباع عناصر G إلى معكوساتها . أثبت أن $xT=x^{-1}$ لكل $x\in G$ وأن G إبدالية .

١٣ - بالرجوع إلى المسألة (١٢) هل تستطيع إيجاد مثال لزمرة منتهية وغير إبدالية ويوجد لها تماثل ذاتي ينقل تماما ثلاثة أرباع عناصرها إلى معكوساتها؟

١٤* - أثبت أنه لأية زمرة منتهية تحتوي على أكثر من عنصرين يوجد تماثل ذاتي غير تافه .

١٥* - لتكن G هي الزمرة التي رتبتها 2n ولنفرض أن رتبة نصف عدد عناصر G هي 2 وأن النصف الآخر يكوّن زمرة جزئية H رتبتها n. أثبت أن رتبة H هي عدد فردي كما أن H زمرة جزئية إبدالية من G.

١٦* - لتكن $\phi(n)$ هي دالة أويلر. إذا كان $a>1$ عددا صحيحا . فأثبت أن $n|\phi(a^n-1)$.

١٧ ـ لتكن G زمرة و Z مركزها فإذا كان T أي تماثل ذاتي على G. فأثبت أن $(Z)T\subset Z$.

١٨ ـ لتكن G زمرة و T تماثلا ذاتيا عليها، ولتكن $N(a)=\{x\in G|xa=ax\}$ لعنصر $a\in G$. أثبت أن $N(aT)=(N(a))T$.

١٩ ـ لتكن G زمرة و T تماثلا ذاتيا عليها و N زمرة جزئية ناظمية في G بحيث يكون $(N)T\subset N$. وضح كيف تستعمل T لتعريف تماثل ذاتي على G/N.

٢٠ ـ استخدم المناقشة التي تلي تمهيدية (٢ـ٨ـ٣) لتكوين:

ا) زمرة غير إبدالية رتبتها = 55.

ب) زمرة غير إبدالية رتبتها = 203.

٢١ ـ لتكن G هي الزمرة التي رتبتها = 9 والمولدة بالعنصرين a و b حيث $a^3=b^3=e$. أوجد جميع التماثلات الذاتية على G.

(٢ ـ ٩) مبرهنة كيلي (Cayley)

عندما نشأت الزمر لأول مرة في الرياضيات فإنها نبعت من مصادر خاصة وفي صيغة ملموسة جدا وغالبا ما كانت على صيغة مجموعة تحويلات نظام رياضي معين.

وفي الواقع إن معظم الزمر المنتهية ظهرت على هيئة تبديلات، أي على هيئة زمر جزئية من S_n ($S_n=A(S)$ حيث S مجموعة منتهية من عناصر عددها n) ولقد كان الرياضي الانجليزي كيلي أول من لاحظ أن كل زمرة يمكن تصورها على هيئة زمرة جزئية من A(S) حيث S مجموعة ما.

وفي هذا البند سنعرض مبرهنة كيلي والنتائج المترتبة عليها.

مبرهنة (٢ـ٩ـ١)

إن أيّة زمرة تُماثل زمرة جزئية من $A(S)$ حيث S مجموعة.

البرهان

لتكن G زمرة. سنستخدم عناصر الزمرة G لتكون هي المجموعة S. وبعبارة

أخرى، $S=G$. إذا كان $g\in G$ فإننا نعرف $\tau_g:S(=G)\to S(=G)$ بالقاعدة $x\tau_g=xg$ لكل $x\in G$.

إذا كان $y\in G$ فإن $y=(yg^{-1})g=(yg^{-1})\tau_g$ أي أن τ_g يطبق S على نفسها. وفضلا عن ذلك فإن τ_g أحادي لأنه إذا كان $x\tau_g=y\tau_g$ فإن $xg=yg$ ومن خاصة الاختزال في الزمر نجد أن هذا يقتضي أن $x=y$. بهذا نكون قد أثبتنا أن $\tau_g\in A(S)$ لكل $g\in G$.

لنعتبر الآن τ_{gh} حيث $g,h\in G$. لأي $x\in G$ نجد أن:

$$x\tau_{gh}=x(gh)=(xg)h=(x\tau_g)\tau_h=x\tau_g\tau_h$$

لاحظ هنا أننا قد استعملنا قانون التجميع. ومن العلاقة $x\tau_{gh}=x\tau_g\tau_h$ نستنتج أن $\tau_{gh}=\tau_g\tau_h$. ولذلك إذا كان $\psi:G\to A(S)$ معرفا بالعلاقة $\psi(g)=\tau_g$ فإن العلاقة $\tau_{gh}=\tau_g\tau_h$ تفيد بأن ψ تشاكل. ما هي نواة ψ ؟

لنفرض أن K نواة ψ عندئذ إذا كان $g_0\in K$ فإن $\psi(g_0)=\tau_{g_0}$ و τ_{g_0} هو التطبيق المحايد على S. لذلك فإنه لأجل $x\in G$ وبصفة خاصة، لأجل $e\in G$ نجد أن $e\tau_{g_0}=e$ بيد أن $e\tau_{g_0}=eg_0=g_0$. وبمقارنة هاتين العلاقتين نستنتج أن $g_0=e$ وبالتالي فإن $K=(e)$، واستنادا إلى نتيجة التمهيدية (٢-٧-٤) نستنتج أن ψ تماثل من G إلى A(S). بهذا نكون قد أثبتنا المبرهنة.

إن هذه المبرهنة تمكننا من أن نعرض أية زمرة مجردة على هيئة زمرة ملموسة، ألا وهي، زمرة تطبيقات، بيد أنها لا تخلو من مواطن الضعف ذلك أنه إذا كانت G زمرة منتهية رتبتها o(G) فإنه بجعل $S=G$ كما ورد ذلك في برهاننا نجد أن A(S) تحتوي على عناصر عددها o(G)!. إن زمرتنا G التي رتبتها o(G) قد فقدت نوعا ما داخل الزمرة A(S) التي بعناصرها التي عددها o(G)! تصبح كبيرة جدا بالمقارنة مع G. والآن نطرح السؤال الآتي: هل نستطيع إيجاد مجموعة S بحيث تكون A(S) أصغر من تلك التي وردت فيما سبق؟ هذا ما سنحاول إنجازه فيما يأتي.

لتكن G زمـرة و H زمـرة جزئية منهـا ولتكن S هي المجمـوعـة التي عناصرها المجموعات المشاركة اليمنى لـ H في G. أي أن $S=\{Hg|g\in G\}$ إنه ليس ضروريا أن تكون S زمرة في حد ذاتها، وفي الواقع، ستكون S زمرة، فقط فيما لو كانت H زمرة جزئية ناظمية في G. ومع ذلك، فإننا نستطيع أن نجعل الزمرة G تؤثر على S بطريقة طبيعية كما يلي:

ليكن $t_g:S\to S$ معـرفـا بالقـاعدة $(Hx)t_g=Hxg$ حيث $g\in G$ وبالعودة إلى إثبات مبرهنة (٢-٩-١) نستطيع أن نبرهن بسهولة على أن

١) $t_g\in A(S)$ لكل $g\in G$

٢) $t_{gh}=t_gt_h$

وهكـذا فإن التـطبيق $\theta:G\to A(S)$ والمعَـرَّف بالقاعدة $\theta(g)=t_g$ هو تشاكل من G إلى A(S). هل بإمكاننا أن نقول إن θ تماثل؟

للإجـابـة على ذلـك نفـرض أن K هي نواة θ. إذا كان $g_0\in K$ فإن العنصر $\theta(g_0)=t_{g_0}$ هو التـطبيق المحـايد على S. وبـالتـالي فإنـه لكـل $x\in S$ يكـون $xt_{g_0}=x$. ولما كان كل عنصر من S هو مجموعة مشاركة يمنى لـ H في G لذلك فإنه يجب أن يكون لدينا $Hat_{g_0}=Ha$ لكل $a\in G$. ومن تعريف t_{g_0}، أي $Hat_{g_0}=Hag_0$ نصل إلى أن $Hag_0=Ha$ لكل $a\in G$.

ومن ناحية أخـرى، إذا كان $b\in G$ بحيث يكـون $Hxb=Hx$ لكـل $x\in G$ فإننا نستطيع إثبات أن $b\in K$. وهكذا فإن $K=\{b\in G|Hxb=Hx$ ، لكل $x\in G\}$.

إننـا بهذا الـوصف لـK ندعي أن K يجب أن تكـون أكـبر زمرة جزئية ناظمية في G محتواة في H. لنوضح أولا ما هو المقصود من كلمة أكبر؟ إننا نعني بذلك أنه إذا كانت N زمرة جزئية ناظمية في G محتواة في H فإن N يجب أن تكون محتواة في K، ونريد أن نثبت أن هذه هي الحالة. إن كون K زمرة جزئية ناظمية في G ينتج من كونها نواة التشاكل على G. إن $K\subset H$ لأنه إذا كان $b\in K$ فإن $Hab=Ha$ لكل $a\in G$ ولذلك وبصورة خاصة، $Hb=Heb=He=H$ ومن ثم فإن $b\in H$.

وأخيرا، إذا كانت N زمرة جزئية ناظمية في G محتواة في H وكان $n \in N$ ، $a \in G$ فإن $ana^{-1} \in N \subset H$ وبالتالي فإن $Hana^{-1}=H$ وهكذا فإن $Han=Ha$ لكل $a \in G$ ولذلك واستنادا إلى تعريف K نجد أن $n \in K$. بهذا نكون قد برهنا.

مبرهنة (٢-٩-٢)

إذا كانت G زمرة و H زمرة جزئية من G وكانت S هي مجموعة كل المجموعات المشاركة اليمنى لـ H في G فإنه يوجد تشاكل θ من G إلى A(S) بحيث تكون نواة θ هي أكبر زمرة جزئية ناظمية في G محتواة في H.

إن مبرهنة كيلي (٢-٩-١) ليست إلا حالة خاصة من هذه المبرهنة وذلك في الحالة التي تكون فيها $H=(e)$. وإذا حدث أن كانت H لا تحتوي على زمرة جزئية ناظمية في G غير (e) فإن θ يجب أن يكون تماثلا من G إلى A(S). وفي هذه الحالة نكون قد قلصنا حجم S المستخدمة في إثبات مبرهنة (٢-٩-١) وهذه الحالة هي الأكثر متعة في الزمر المنتهية. ومن أجل ذلك، سنستعمل هذه الملاحظة كوسيلة لإثبات احتواء زمرة منتهية معينة على زمرة جزئية ناظمية غير تافهة وأيضا كوسيلة لتمثيل زمر منتهية معينة على هيئة زمر تبديلات على مجموعات صغيرة.

الآن ندرس هاتين الملاحظتين عن كثب. لنفرض أن G تحتوي على زمرة جزئية H التي دليلها i(H) (أي عدد المجموعات المشاركة اليمنى لـ H في G) يحقق المتراجحة $i(H)!<0(G)$ ولتكن S هي مجموعة المجموعات المشاركة اليمنى لـ H في G.
إن التطبيق θ الوارد في المبرهنة (٢-٩-٢) لا يمكن أن يكون تماثلا، لأنه لو كان كذلك، لكانت θ(G) تحتوي على عناصر عددها o(G) ومع ذلك فهي زمرة جزئية من A(S) التي عدد عناصرها $i(H)!$ حيث $o(G)>i(H)!$ ولذلك فإن نواة θ يجب أن تكون أكبر من (e).
ونظرا لأن النواة هي أكبر زمرة جزئية ناظمية في G محتواة في H، فإننا نستنتج من ذلك أن H تحتوي على زمرة جزئية ناظمية غير تافهة في G.
ومع ذلك، فإن للمناقشة الواردة آنفا مقتضيات حتى ولو كانت $i(H)!$ ليست أصغر من o(G). فإذا كانت $i(H)!$ لا تقبل القسمة على o(G) فإنه بالرجوع إلى مبرهنة

لاجرانج نجد أن $A(S)$ لا تحتوي على زمرة جزئية رتبتها $o(G)$ ومن ثم فإنه لا توجد زمرة جزئية من $A(S)$ تماثل G ، بيد أن $A(S)$ تحوي $\theta(G)$ ولذلك فإن $\theta(G)$ لا يمكن أن تماثل G وبعبارة أخرى، لا يمكن أن يكون θ تماثلا ولكن H في هذه الحالة، كما رأينا آنفا، تحتوي على زمرة جزئية ناظمية غير تافهة.

نلخص ما سبق بالتمهيدية الآتية.

تمهيدية (٢-٩-١)

إذا كانت G زمرة منتهية وكانت H زمرة جزئية من G ، $H \neq G$ بحيث تكون $o(G) \nmid i(H)!$ فإن H يجب أن تحتوي على زمرة جزئية ناظمية غير تافهة في G. وبصورة خاصة لا يمكن أن تكون G زمرة بسيطة.

تطبيقـــات

(١) لتكن G زمرة رتبتها 36 ولنفرض أن G تحتوي على زمرة جزئية H رتبتها 9 (سنرى فيما بعد أن هذه هي الحالة دائما) عندئذ $i(H)=4$ كما أن $4!=24<36=o(G)$ ولـــذلـــك فإن H يجب أن تحتـوي على زمـرة جزئية ناظمية $N\neq(e)$ في G بحيث إن $o(N)|9$ ، وبعبارة أخرى، إن رتبة N هي 3 أو 9.

(٢) لتكن G زمرة رتبتها 99 ولنفرض أن H زمرة جزئية من G رتبتها 11 (سنرى فيما بعد أن هذا يجب أن يكون صحيحا). عندئذ $i(H)=9$ ولما كان $99 \nmid 9!$ لذلك فإنه يوجد زمرة جزئية ناظمية غير تافهة N في G ، $H \supset N$ وحيث إن $o(H)=11$ هو عدد أولي لذا فإن H لا تحتوي على زمر جزئية غير نفسها والزمرة الجزئية التافهة (e) وبناءً على ذلك فإن $N=H$ الأمر الذي يقتضي أن H نفسها زمرة جزئية ناظمية في G.

(٣) لتكن G زمرة غير إبدالية رتبتها 6. استنادا إلى مسألة (١١) بند (٢ ـ ٣)، يوجـد عنصر $a\neq e$ في G بحيث يكون $a^2=e$ وعليه فإن رتبة الزمرة الجزئية $H=\{e,a\}$

تساوي 2 كما أن $i(H)=3$. لنفرض، مؤقتا، أننا نعلم أن H ليست ناظمية في G. لما كانت H لا تحتوي على زمر جزئية غير نفسها و (e) ، لذا فإن H لا تحتوي على زمر جزئية ناظمية في G. وبناء عليه فإن G متماثلة مع زمرة جزئية T من $A(S)$ رتبتها 6 حيث S هي مجموعة المجموعات المشاركة اليمنى لـ H في G. ولما كان $o(A(S))=i(H)!=3!=6$ لذا فإن $T=S_3$، وبعبارة أخرى، فإن $G\approx A(S)\approx S_3$.

لقد أثبتنا أن أية زمرة غير إبدالية رتبتها تساوي 6 متماثلة مع S_3. كل ما بقي لدينا هو إثبات أن H ليست ناظمية في G. وحيث إن هذا قد لا يخلو من فائدة، لذلك فإننا نبرهن هذا بالتفصيل. فلو كانت $H=\{e,a\}$ ناظمية في G لكان $gag^{-1}\in H$ لكل $g\in G$ وكان $gag^{-1}\neq e$ مما يجعل $gag^{-1}=a$ أو بعبارة أخرى $ga=ag$ لكل $g\in G$ ليكن $b\in G$ و $b\notin H$. ولنعتبر $N(b)=\{x\in G|xb=bx\}$. إن $N(b)$ زمرة جزئية من G وفقا لمسألة سابقة كما أن $N(b)\supset H$ و $N(b)\neq H$ لأن $b\in N(b)$ و $b\notin H$. ولما كانت H زمرة جزئية من $N(b)$ لذا فإن $o(H)|o(N(b))|6$. إن العدد الزوجي الوحيد n حيث $2<n\leqslant 6$ والذي يقسم 6 هو 6 نفسه لذا فإن $o(N(b))=6$ وبناء عليه فإن b يتبادل مع جميع عناصر G. لذا فإن كل عنصر من G يتبادل مع أي عنصر آخر من G مما يترتب عليه أن G إبدالية وهذا يناقض الفرض ولهذا فإنه لا يمكن أن تكون H زمرة جزئية ناظمية في G. إن هذا البرهان طويل إلى حد ما بيد أنه يوضح بعض الأفكار التي طوِّرت حتى هذه المرحلة.

مسائل

١ - لتكن G زمرة ثم اعتبر التطبيقات λ_g من G إلى نفسها حيث $g\in G$ والمعرفة بالقاعدة $x\lambda_g=gx$ لكل $x\in G$. أثبت أن λ_g أُحاديّ وغامر وأن $\lambda_{gh}=\lambda_h\lambda_g$.

٢ - ليكن λ_g معرفا كما في المسألة الأولى و τ_g معرفا كما ورد في إثبات مبرهنة (٢-٩-١).
أثبت أن التطبيقين λ_g و τ_h يحققان العلاقة $\lambda_g\tau_h=\tau_h\lambda_g$ وذلك لأي عنصرين g و h في G. [إرشاد: اعتبر $x(\lambda_g\tau_h)$ و $x(\tau_h\lambda_g)$ حيث $x\in G$].

٣ - إذا كان θ تطبيقا أُحاديًا من G على نفسها بحيث يكون $\lambda_g\theta=\theta\lambda_g$ لكل $g\in G$.
فأثبت أن $\theta=\tau_h$ حيث إن h عنصر ما من G.

٤ - (أ) إذا كانت H زمرة جزئية من G . فأثبت أن gHg^{-1} زمرة جزئية من G وذلك لكل $g\in G$.

(ب) أثبت $W=\bigcap_{g\in G} gHg^{-1}$ هي زمرة جزئية ناظمية في G.

٥ - باستخدام تمهيدية (٢-٩-١) برهن على أن كل زمرة رتبتها p^2 حيث p عدد أولي يجب أن تحتوي على زمرة جزئية ناظمية رتبتها p.

٦ - إذا كانت رتبة G هي p^2 فأثبت أن أية زمرة جزئية ناظمية رتبتها p يجب أن تكون محتواة في مركز G.

٧ - باستخدام مسألة (٦) أثبت أن أية زمرة رتبتها p^2 هي زمرة إبدالية.

٨ - إذا كان p عددا أوليا. فأثبت أن أية زمرة رتبتها 2p يجب أن تحتوي على زمرة جزئية رتبتها p وأن هذه الزمرة الجزئية ناظمية في G.

٩ - إذا كانت $o(G)=pq$ ، حيث إن p و q عددان أوليان مختلفان، وكانت G تحتوي على زمرتين جزئيتين ناظميتين رتبة كل منهما p و q على الترتيب. فأثبت أن G دورية.

١٠ - لتكن $o(G)=pq$ ، حيث إن p و q عددان أوليان و $p>q$، أثبت أن:

(ا) G تحتوي على زمرتين جزئيتين رتبة كل منهما p و q على الترتيب.

(ب) إذا كان $q\nmid p-1$ فإن G دورية.

(جـ) إذا كان p و q عددين أوليين وكان $q|p-1$ فإنه يوجد زمرة غير إبدالية رتبتها pq.

(د) أية زمرتين غير إبداليتين رتبتاهما pq متماثلتان.

(٢ - ١٠) زمر التبديلات

لقد رأينا أن كل زمرة يمكن تمثيلها كزمرة جزئية من A(S) حيث S هي أية مجموعة. وبصورة خاصة، يمكن أن تمثل أية زمرة منتهية كزمرة جزئية من S_n حيث n عدد صحيح موجب و S_n هي زمرة التناظر من الدرجة n. إن هذا يظهر بوضوح أن الزمرة S_n نفسها تستحق دراسة أكثر عمقا.

لنفرض أن S مجموعة منتهية تحتوي على عناصر عددها n هي $x_1,x_2,...,x_n$ إذا كان $\phi \in A(S)=S_n$ فإن ϕ تطبيق أُحادِيّ من S على نفسها ونستطيع كتابة ϕ صراحة وذلك بتوضيح تأثيره على كل عنصر فمثلا $\phi: x_1 \to x_2, x_2 \to x_4, x_4 \to x_3, x_3 \to x_1$ ولكن الكتابة على هذا النحو صعبة إلى حد ما وبدلا من ذلك فإنه يمكن كتابة ϕ بطريقة مختصرة كما يلي :

$$\begin{pmatrix} x_1\, x_2\, x_3 \ldots\ldots x_n \\ x_{i_1}\, x_{i_2}\, x_{i_3} \ldots\ldots x_{i_n} \end{pmatrix}$$

حيث x_{i_k} هي صورة العنصر x_i تحت تأثير ϕ وبالعودة إلى مثالنا الآنف الذكر فإنه يمكن تمثيل ϕ كما يلي :

$$\begin{pmatrix} x_1\, x_2\, x_3\, x_4 \\ x_2\, x_4\, x_1\, x_3 \end{pmatrix}$$

ومع أن كتابة ϕ بهذه الطريقة أسهل قليلا فإنها لا تخلو من الإطالة ذلك لأن استخدام الرمز x لا يخدم أي غرض، إذ أنه باستطاعتنا كتابة التبديل على الشكل الآتي :

$$\begin{pmatrix} 1\, 2 \ldots\ldots n \\ i_1\, i_2 \ldots\ldots i_n \end{pmatrix}$$

وبهذه الطريقة يمكن أن نكتب مثالنا السابق كما يلي :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

إذا كان θ و ψ تبديلين في S_n فكيف تمثل $\theta\psi$ وفقا لهذه الطريقة؟

لحساب هذا نرى أولا ما هو تأثير $\theta\psi$ على x_1 (الذي سنكتبه على شكل 1). إن θ يرسل 1 إلى i_1 بينما ψ يرسل i_1 إلى k مثلا . وبالتالي فإن $\theta\psi$ يرسل 1 إلى k ثم نكرر هذه الطريقة على الأعداد 2,3,...n. فمثلا إذا كان θ هو التبديل :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

وكان ψ هو التبديل

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

فإن $i_1=3$ و ψ يرسـل 3 إلى 2 ومن ثم فإن $k=2$ وعليه فإن $\theta\psi$ ينقـل 1 إلى 2 وبـالمثل $2\to1, 3\to3, 4\to4$ أي أن تمثيل $\theta\psi$ هو:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

فإذا كتبنا

$$\theta=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

و

$$\psi=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

فإن

$$\theta\psi=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

إن هذه هي الطريقة التي سنتبعها في ضرب الرموز من الصيغة

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},\ \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

لتكن S مجموعة، $\theta\in A(S)$ ولنفرض أن $a,b\in S$ ، عندئذ نعرف $a\equiv_\theta b$ إذا وفقط إذا كان $b=a\theta^i$ حيث i عدد صحيح (قد يكون i موجبا أو سالبا أو صفرا) إننا ندعي أن هذه هي علاقة تكافؤ على S وذلك لأن:

(١) $a\equiv_\theta a$ لأن $a=a\theta^0=ae$

(٢) إذا كان $a\equiv_\theta b$ فإن $b=a\theta^i$ ومن ثم فإن $a=b\theta^{-i}$ وبناء عليه $b\equiv_\theta a$.

(٣) إذا كان $a\equiv_\theta b$ و $b\equiv_\theta c$ فإن $b=a\theta^i$ و $c=b\theta^j=(a\theta^i)\theta^j=a\theta^{i+j}$ وهـذا يقـتضي أن $a\equiv_\theta c$.

إن علاقة التكافؤ هذه تفرق المجموعة S إلى مجموعات جزئية منفصلة أي إلى فصول تكافؤ وذلك استنادا إلى مبرهنة (١-١-١). كما نطلق على فصل التكافؤ الذي يمثله العنصر $s\in S$ **مـدار** (Orbit) s بالنسبة إلى θ أي أن مدار s بالنسبة إلى θ يتكون

من جميع العناصر $s\theta^i$ حيث $i=0,\pm1,...$. وبصورة خاصة، إذا كانت S مجموعة منتهية و $s\in S$ فإنه يوجد عدد موجب أصغر $l=l(s)$ يعتمد على s بحيث يكون $s\theta^l=s$. إن مدار s بالنسبة إلى θ يتكون عندئذ من جميع العناصر $s,s\theta,s\theta^2,...,s\theta^{l-1}$. نعرف **دورة** θ (cycle) بأنها المجموعة المرتبة $(s,s\theta,...,s\theta^{l-1})$. إن بإمكاننا تعيين θ متى ما عرفنا جميع دوراته ذلك لأننا سنعرف صورة أي عنصر تحت تأثير θ ونوضح هذه الأفكار بمثال قبل أن نستطرد في الموضوع.

ليكن

$$\theta=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 1 & 3 & 5 & 6 & 4\end{pmatrix}$$

حيث تتكون S من العناصر 1,2,...,6 (تذكر أن 1 يرمز للعنصر x_1 و 2 يرمز للعنصر x_2 وهكذا...). وبدءا بالعنصر 1 نجد أن مدار 1 يتكون من $1=1\theta^\circ, 1\theta^1=2, 1\theta^2=2\theta=1$ وبالتالي فإن مدار 1 هو المجموعة {1,2}. ومن هنا نستنتج أن مدار 2 هو المجموعة نفسها. إن مدار 3 يتكون فقط من 3. كما أن مدار 4 يتكون من4، $5=4\theta$، $6=5\theta=4\theta^2$، $4=6\theta=(4\theta^2)\theta=4\theta^3$ وبالتالي فإن دورات θ هي (1,2),(3),(4,5,6).

الآن نحيد قليلا عن مثالنا المحدد θ. ولنفرض أن الدورة $(i_1,i_2,...,i_r)$ تعني التبديل ψ الذي يرسل i_1 إلى i_2 و i_2 إلى i_3 و... و i_{r-1} إلى i_r و i_r إلى i_1 ويترك جميع العناصر الأخرى في S ثابتة. وهكذا.

على سبيل المثال، إذا كانت S تتكون من العناصر 1,2,...,9 فإن الرمز (1,3,4,2,6) يعني التبديل

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9\end{pmatrix}$$

إن ضرب الدورات يتم بضرب التبديلات التي تمثلها.

ومرة أخرى، إذا كانت S تحتوي على 9 عناصر فإن

$$(1\ 2\ 3)\,(5\ 6\ 4\ 1\ 8)=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&2&3&1&6&4&7&5&9\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&8&1&6&4&7&5&9\end{pmatrix}$$

لنعود الآن إلى الأفكار المطروحة في الفقرة السابقة لهذه الفقرة، ولنطرح السؤال الآتي: إذا كان لدينا التبديل:

$$\theta= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

فما هي دورات θ ؟

أولا نوجد مدار 1 ، أي

$$1, 1\theta=2, 1\theta^2=2\theta=3, 1\theta^3=3\theta=8, 1\theta^4=8\theta=5, 1\theta^5=5\theta=6, 1\theta^6=6\theta=4, 1\theta^7=4\theta=1$$

أي أن مدار 1 هو المجموعة $\{1,2,3,8,5,6,4\}$.

كما أن مداري 7 و 9 هما $\{7\}$ و $\{9\}$ على الترتيب. وهكذا فإن دورات θ هي:

$$(7), (9), (1,1\theta,1\theta^2,\ldots,1\theta^6) =(1,2,3,8,5,6,4)$$

وعلى القارىء التحقق من أنه إذا ضرب الدورات $(9),(7),(1,2,3,8,5,6,4)$ (كما هو معرف في الفقرة السابقة) فإنه سيحصل على θ أي أن θ في هذه الحالة، على الأقل، هو حاصل ضرب دوراته.

لكن هذا ليس من قبيل المصادفة ذلك أنه يمكن ببساطة برهان التمهيدية الآتية.

تمهيدية (٢-١٠-١)

كل تبديل هو عبارة عن حاصل ضرب دوراته.

البرهان:

ليكن θ تبديلا، عندئذ تأخذ دورات θ الصيغة $(s,s\theta,\ldots,s\theta^{l-1})$.

استنادا إلى تعريف ضرب الدورات، كما ورد سابقا، وحيث إن دورات θ منفصلة لذا فإن صورة $s' \in S$ تحت تأثير θ التي هي $s'\theta$ ، هي نفس صورة s'

تحت تأثير ψ حيث ψ هو حاصل ضرب دورات θ المختلفة، وبالتالي فإن تأثير θ على كل عنصر من عناصر S هو نفس تأثير ψ ، أي أن $\psi=\theta$ وهذا هو المطلوب برهانه .

إذا كانت الملاحظات الواردة فيما سبق لا تزال غير واضحة فإنه يجب على القارىء أن يأخذ تبديلا معينا ثم يوجد دوراته، وبعد ذلك يأخذ حاصل ضرب هذه الدورات ليتحقق من التمهيدية، وعندما يفعل هذا فإن التمهيدية ستصبح واضحة لديه .
من المعتاد كتابة نص **التمهيدية** (٢-١٠-١) على الصيغة التالية *«إن كل تبديل يمكن التعبير عنه بطريقة وحيدة على هيئة حاصل ضرب دورات منفصلة»* .

لنعتبر الدورة $(1,2,3,...,m)$ التي طولها m. إنه يمكن بحسابات بسيطة إثبات أن :

$$(1,2,3,...m) = (1,2)\,(1,3),...\,(1,m)$$

وعموما فإن الدورة $(a_1,a_2,...\,a_m)$ التي طولها m تساوي $(a_1,a_2)(a_1,a_3),...\,(a_1,a_m)$.
إن هذا التفريق غير وحيد ونعني بذلك أن الدورة التي طولها m يمكن كتابتها كحاصل ضرب دورات طول كل منها 2 بأكثر من طريقة،
فمثلا

$$(1,2,3) = (1,2)(1,3) = (3,1)(3,2)$$

الآن، لما كان كل تبديل هو عبارة عن حاصل ضرب دورات منفصلة وحيث إن كل دورة عبارة عن حاصل ضرب دورات طول كل منها 2 فإننا نكون قد برهنا على التمهيدية الآتية .

تمهيدية (٢-١٠-٢)

كل تبديل هو حاصل ضرب دورات طول كل منها 2.

سوف نطلق على الدورة التي طولها 2 **بالمناقلة** (Transposition)

تعريف

*يقال عن التبديل $\theta \in S_n$ **إنه تبديل زوجي (Even)** إذا أمكن تمثيله على هيئة حاصل ضرب مناقلات عددها زوجي.*

إن التعريف الوارد فيما سبق يوضح أن للتبديل θ تمثيل على هيئة حاصل ضرب عدد زوجي من المناقلات ولكن قد يكون له تمثيلات أخرى على هيئة حاصل ضرب عدد فردي من التبديلات ونريد هنا أن نبين أن هذا لا يمكن أن يحدث.
إننا، بصراحة، غير راضين عن البرهان الذي سنقدمه لهذه الحقيقة ذلك لأنه يستخدم كثيرات الحدود الأمر الذي يبدو غريبا على الموضوع المطروح.

لنعتبر كثيرة الحدود في المتغيرات التي عددها n

$$p(x_1,x_2,\ldots,x_n)=\prod_{i<j}(x_i-x_j)$$

ولنعتبر أن $\theta \in S_n$ يؤثر على كثيرة الحدود $p(x_1,x_2,\ldots,x_n)$ وفق القاعدة

$$\theta:p(x_1,x_2,\ldots x_n)=\prod_{i<j}(x_i-x_j) \rightarrow \prod_{i<j}(x_{\theta(i)}-x_{\theta(j)})$$

إن من الواضح أن:

$$\theta:p(x_1,x_2,\ldots,x_n) \rightarrow \pm p(x_1,x_2\ldots x_n)$$

فعلى سبيل المثال، إن التبديل $\theta=(134)(25)$ في S_5 ينقل

$$p(x_1,\ldots x_5)=(x_1-x_2)(x_1-x_3)\ (x_1-x_4)(x_1-x_5)(x_2-x_3)(x_2-x_4)\ (x_2-x_5)(x_3-x_4)(x_3-x_5)(x_4-x_5)$$

إلى:

$$(x_3-x_5)(x_3-x_4)\ (x_3-x_1)(x_3-x_2)(x_5-x_4)(x_5-x_1)(x_5-x_2)(x_4-x_1)(x_4-x_2)(x_1-x_2)$$

والتي يمكن التأكد من أنه يساوي $-p(x_1,\ldots x_5)$.

وبصفة خاصة، إذا كان θ **مناقلة** فإن:

$$\theta:p(x_1,\ldots,x_n) \rightarrow -\ p(x_1,\ldots,x_n)$$

(تحقق من ذلك).

وهكـذا إذا أمكن تمثيل التبـديل π كحاصل ضرب مناقلات عددها زوجي، فإن π يجب أن يبقى $p(x_1,...x_n)$ ثابتا، ولذلك فإن أي تمثيل لـ π على هيئة حاصل ضرب منـاقلات يجب أن يبقى $p(x_1,...x_n)$ ثابتا وبعبارة أخرى، في أي تمثيل لـπ على هيئة حاصـل ضرب منـاقلات يجب أن يكون عدد المناقلات زوجيًّا. إن هذا يوضح أن تعريف التبديل الزوجي ذو معنى. إن التبديل غير الزوجي يسمى تبديلا **فرديا** (odd).

إن الحقائق الآتية واضحة الآن:

(١) حاصل ضرب تبديلين زوجيين هو تبديل زوجي.

(٢) حاصل ضرب تبديلين أحدهما زوجي والآخر فردي هو تبديل فردي.

(٣) حاصل ضرب تبديلين فرديين هو تبديل زوجي.

إن قاعـدة تركيب تبديل زوجي مع فردي مماثلة لتركيب عدد زوجي مع عدد فردي بالنسبة لعملية الجمع. إن هذا ليس من قبيل المصادفة ذلك أن القاعدة الأخيرة مستعملة في برهان الحقائق الثلاث الآنفة الذكر.

لتكن A_n هي مجموعة كل التبديلات الزوجية في S_n وحيث إن حاصل ضرب تبديلين زوجيين هو زوجي لذلك فإنه يجب أن تكون A_n زمرة جزئية من S_n. إننا ندَّعي أنها ناظمية في S_n. إن أفضل طريقة لبرهان ذلك قد تكون الطريقة الآتية.

لتكـن W هي الـزمـرة $\{1,-1\}$ بالـنسبـة لعملية ضرب الأعـداد الحقيقية ولنعـرف $\psi:S_n\to W$ وفْق القـاعـدة $\psi(s)=1$ إذا كان s زوجيا و $\psi(s)=-1$، إذا كان s فرديا. إن ψ تشاكل من S_n على W وذلك بناء على القواعد ١، ٢، ٣ الواردة فيما سبق. كما أن نواة ψ هي تمامـا A_n وحيث إن A_n هي نواة التشـاكـل لذا فإنها ناظمية في S_n واستنادا إلى مبرهنة (٢-٧-١) فإن $S_n/A_n\approx W$ وحيث إن

$$2=o(W)=o(\frac{S_n}{A_n})=\frac{o(S_n)}{o(A_n)}$$

لذا فإن $o(A_n)=\frac{1}{2}n!$. إن A_n تدعى **بالزمرة المتناوبة** (Alternating) من الدرجة n.

إن الملاحظات السابقة يمكن تلخيصها بالتمهيدية الآتية .

تمهيدية (٢-١٠-٣)

إن S_n تحتوي على زمرة جزئية ناظمية دليلها 2 وهذه الزمرة هي الزمرة المتناوبة A_n المكونة من جميع التبديلات الزوجية .

سنعود إلى S_n مرة أخرى وذلك عند نهاية البند القادم .

مسائل

١ - أوجد مدارات ودورات التبديلين الآتيين :

(ا) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$

(ب) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$

٢ - اكتب التبديلين الواردين في المسألة السابقة كحاصل ضرب دورات منفصلة .

٣ - عبر عن التبديلين الآتيين كحاصل ضرب دورات منفصلة :

(أ) $(1,2,3)(4,5)(1,6,7,8,9)(1,5)$

(ب) $(1,2)(1,2,3)(1,2)$

٤ - برهن على أن

$$(1,2,\ldots,n)^{-1} = (n,n-1,n-2,\ldots,2,1)$$

٥ - أوجد البنية الدورية لجميع قوى التبديل $(1,2,\ldots,8)$.

٦ - (أ) ما هي رتبة الدورة التي طولها m.

(ب) ما هي رتبة حاصل ضرب الدورات المنفصلة التي أطوالها $m_1,m_2,\ldots m_k$ ؟

(جـ) كيف توجد رتبة تبديل معطى؟

٧ - احسب $a^{-1}ba$ حيث :

(ا) $a=(1,2,5)(1,2),\ b=(1,5,7,9)$

(ب) $a=(5,7,9),\ b=(1,2,3)$

٨ - (أ) إذا أعطيت التبديلين $x=(1,2)(3,4)$, $y=(5,6)(1,3)$ فأوجد تبديلا a بحيث يكون $a^{-1}xa=y$.

(ب) برهن على أنه لا يوجد تبديل a بحيث يكون

$$a^{-1}(1,2,3)a=(1,3)(5,7,8)$$

(جـ) برهن على أنه لا يوجد تبديل a بحيث يكون $a^{-1}(1,2)a=(3,4)(1,5)$.

٩ - عين العدد m الذي من أجله تكون الدورة التي طولها m زوجية.

١٠ - عين أيا من التبديلات الآتية هي تبديل زوجي

(أ) $(1,2,3)(1,2)$

(ب) $(1,2,3,4,5)(1,2,3)(4,5)$

(جـ) $(1,2)(1,3)(1,4)(2,5)$

١١ - برهن على أن أصغر زمرة جزئية في S_n تحوي $(1,2)$ و $(1,2,\ldots,n)$ هي S_n (بعبارة *أخرى:* أثبت أن هذين التبديلين يولدان S_n).

١٢* - برهن على أنه إذا كان $n\geqslant3$ فإن الزمرة الجزئية المولدة بالدورات التي طولها 3 هي A_n.

١٣* - برهن على أنه إذا كانت A_n تحتوي على زمرة ناظمية بحيث تحوي هذه الزمرة الجزئية الناظمية دورة طولها 3 فإن هذه الزمرة الجزئية الناظمية هي نفسها A_n.

١٤* - برهن على أن A_5 لا تحتوي على زمرة ناظمية N بحيث تكون $A_5\neq N\neq(e)$.

١٥* - مع افتراض نتيجة مسألة (١٤) برهن على أن رتبة أية زمرة جزئية من A_5 هي على الأكثر 12.

١٦ - أوجد جميع الزمر الجزئية الناظمية في S_4.

١٧* - إذا كان $n\geqslant5$ فبرهن على أن A_n هي الزمرة الجزئية الناظمية الوحيدة غير التافهة في S_n.

تؤكد مبرهنة كيلي (مبرهنة ٢-٩-١) على أن كل زمرة تُماثل زمرة جزئية في $A(S)$ حيث S مجموعة ما. وبصفة خاصة، نقول إنه يمكن تمثيل كل زمرة منتهية على أنها زمرة تبديلات. دعنا نطلق على هذا التمثيل كما وارد في إثبات المبرهنة (٢-٩-١) **بالتمثيل التبديلي** (Permutation Representation) للزمرة G.

١٨ ـ أوجد التمثيل التبديلي للزمرة الدورية من الرتبة ١٦ .

١٩ ـ لتكن G هي الزمرة {e,a,b,ab} التي رتبتها 4 حيث $a^2=b^2=e$ و $ab=ba$.

أوجد التمثيل التبديلي للزمرة G.

٢٠ ـ لتكن G هي الزمرة S_3. أوجد التمثيل التبديلي للزمرة S_3 (ملاحظة: إن هذا يعطي تماثلا من S_3 إلى S_6).

٢١ ـ لتكن G هي الزمرة $\{e,\theta,a,b,c,\theta a,\theta b,\theta c\}$ حيث

$$a^2=b^2=c^2=\theta,\ \theta^2=e,\ ab=\theta ba=c,\ bc=\theta cb=a,\ ca=\theta ac=b$$

(ا) أثبت أن θ ينتمي إلى مركز G أي Z وأن $Z=\{e,\theta\}$.

(ب) أوجد زمرة المبدلات الجزئية في G.

(جـ) أثبت أن كل زمرة جزئية من G هي ناظمية .

(د) أوجد التمثيل التبديلي للزمرة G.

(ملاحظة: تدعى G غالبا بزمرة **الوحدات الرباعية** (Quaternion Units) كما أنها مع الأنظمة الجبرية المترتبة عليها ستظهر في هذا الكتاب) .

٢٢ ـ لتكن G هي الزمرة الزوجية من الرتبة 2n (انظر مسألة ١٧ بند ٢ ـ ٦) .

أوجد التمثيل التبديلي للزمرة G.

(دعنا نطلق على تمثيل زمرة G كمجموعة تبديلات والواردة في مسألة (١) بند (٢ـ٩) **بالتمثيل التبديلي الثاني**) .

٢٣ ـ أثبت أنه إذا كانت G زمرة إبدالية فإن التمثيل التبديلي للزمرة G يتطابق مع التمثيل التبديلي الثاني لها (أي أنه وفْقا لاصطلاحات البند السابق، $\lambda_g=\tau_g$ لكل $g\in G$).

٢٤ ـ أوجد التمثيل التبديلي الثاني للزمرة S_3. تحقق من أن التبديلات التي تحصل عليها هنا وتلك الواردة في المسألة (٢٠) تحقق العلاقة $\lambda_a\tau_b=\tau_b\lambda_a$ لكل a و b في S_3.

٢٥ ـ أوجد التمثيل التبديلي الثاني للزمرة G المعرفة في المسألة (٢١) .

٢٦ ـ أوجد التمثيل التبديلي الثاني للزمرة الزوجية التي رتبتها 2n.

لتكن H زمرة جزئية من G ولنطلق على التطبيق t_g حيث $g\in G$ والمعرف في المناقشة الواردة قبل مبرهنة (٢ـ٩ـ٢) **التمثيل المشارك** (Coset representation)

للزمـرة G بواسـطة H. إن هذا يمثـل G على أنها زمرة تبديلات بيد أنه ليس بالضرورة أن يكون هذا التطبيق تماثليا وإنما تطبيقا تشاكليا فقط (انظر مبرهنة ٢-٩-٢).

٢٧ - لتكن $G=(a)$ الزمرة الدورية التي رتبتها 8 ولتكن $H=(a^4)$ زمرة جزئية من G والتي رتبتها 2. أوجد التمثيل المشارك للزمرة G بواسطة G.

٢٨ - لتكن G هي الـزمـرة الـزوجية التي رتبتهـا 2n والمولدة بالعنصرين a,b بحيث يكـون $a^2=b^n=e$ و $ab=b^{-1}a$ ولـتـكن $H=\{e,a\}$. أوجـد التمثيل المشـارك للزمرة G بواسطة H.

٢٩ - لتكن G هي الـزمرة الواردة في المسألة (٢١) ولتكن $H=\{e,\theta\}$. أوجد التمثيل المشارك لهذه الزمرة بواسطة H.

٣٠ - لتكن G هي الـزمـرة S_n ، أي زمـرة التنـاظر من الدرجة n ، والتي باعتبارها تبديلات تؤثر على المجموعة $\{1,2,\ldots,n\}$ ولتكن $H=\{\sigma\in G: n\sigma=n\}$.

(ا) برهن على أن H تماثل S_{n-1}.

(ب) أوجد مجموعة العناصر $a_1,\ldots,a_n\in G$ بحيث تكون $Ha_1,\ldots,Ha_n$ هي كل المجموعات المشاركة اليمنى لـ H في G.

(جـ) أوجد التمثيل المشارك للزمرة G بواسطة H.

(٢ - ١١) مبـدأ آخـر للعـد

إن الـرياضيات غنيَّة بأسـاليب الـبرهـان. ووفق هذا التنـوع الكبير يبدو مبدأ العـد أمـراً سهـلاً ومع هذا فإن مبدأ العد من الأمور الأكثر صعوبة. بالطبع، إننا لا نقصد بالعد وضع جداول اللوغاريثمات أو جداول الجمع بل إنما نقصد به أنه عملية حسابية دقيقة لجميع الاحتمالات في حالات معقدة جدا. إنه يمكن عمل ذلك بصورة قسرية بالتعامل مع كل حالة على انفراد ولكن هذه الطريقة غالبا ما تكون مملة ومُعوِّقة للتفكـير الـرياضي. لذلـك، فمن الأفضـل أن نهون على أنفسنـا عند معالجة هذا الموضوع. وفي الحقيقة، أن اعتراضنا على التعامل مع كل حالة على انفراد هو أن هذه الطريقة لا تصلح إلا للنادر من عمليات العد. لهذا فإننا نجد في مجالات متعددة في

الرياضيات أساليب عد جميلة تفيدنا بالضبط عن عدد العناصر التي تحقق شروطا معينة ويفضل الرياضيون طريقة العد التي تحسب أمورا معينة بطريقتين مختلفتين وبمقارنة هاتين الطريقتين يحصلون على استنباطات محددة.

وبصفة عامة، يمكن تعريف علاقة تكافؤ على مجموعة منتهية وحساب عدد عناصر فصول التكافؤ وفق هذه العلاقة ثم مساواة عدد العناصر في المجموعة بمجموع رتب فصول التكافؤ. إن هذه الطريقة ستتضح لنا في هذا البند، بمعنى أننا سنقدم علاقة ونثبت أنها علاقة تكافؤ ثم نوجد وصفا جبريا دقيقا لسعة كل فصل تكافؤ ومن هذا الوصف البسيط سنخرج بنتائج دقيقة وقوية للزمر المنتهية.

تعريف

إذا كان $a,b\in G$ فإنه يقال إن العنصر b ***مرافق*** *(conjugate) للعنصر a إذا وجد عنصر $c\in G$ بحيث يكون $b=c^{-1}ac$.* وهنا، سنكتب $a\sim b$ وسنشير إلى هذه العلاقة على أنها علاقة **الترافق** (conjugacy).

تمهيدية (٢-١١-١)

إن علاقة الترافق هي علاقة تكافؤ على G.

البرهان

كما هو متبع، لكي نثبت أن هذه هي علاقة تكافؤ يجب أن نثبت ما يلي:

(١) $a\sim a$.

(٢) $a\sim b$ يقتضي أن $b\sim a$.

(٣) $a\sim b$ و $b\sim c$ يقتضي أن $a\sim c$ لكل a,b,c في G.

ونبدأ بإثبات كل واحدة على انفراد

(١) لما كان $a=e^{-1}ae$ لذا فإن $a\sim a$، حيث يقوم e مقام c في تعريف الترافق.

(٢) إذا كان $a\sim b$ فإن $b=x^{-1}ax$ حيث $x\in G$ ومن ثم فإن $a=(x^{-1})^{-1}b(x^{-1})$ وحيث إن $y=x^{-1}\in G$ و $a=y^{-1}by$ لذا فإنه ينتج أن $b\sim a$.

(٣) لنفرض أن $a\sim b$ و $b\sim c$ حيث $a,b,c\in G$ عندئذ $b=x^{-1}ax$ و $c=y^{-1}by$ حيث $x,y\in G$. بالتعويض عن b بالتعبير $c=y^{-1}by$ نحصل على $c=y^{-1}(x^{-1}ax)y=(xy)^{-1}a(xy)$ وحيث إن $xy\in G$ لذا فإننا نستنتج أن $a\sim c$.

ليكن $C(a)=\{x\in G|a\sim x\}$ هو فصل التكافؤ للعنصر $a\in G$ وفق هذه العلاقة ويدعى عادة **فصل الترافق** للعنصر $a\in G$. إنه يتكون من مجموعة العناصر المختلفة من الصيغة $y^{-1}ay$ حيث y تمر على جميع عناصر G.

إن اهتمامنا يتركز، الآن، على الحالة التي تكون عندها G منتهية. لنفرض أن $C(a)$ يحتوي على عناصر عددها c_a ولنبحث عن وصف آخر للعدد c_a. ولكن قبل أن نفعل ذلك نلاحظ أن $o(G)=\Sigma c_a$ حيث يتم الجمع على المجموعة المكونة من ممثلي فصول الترافق. هذه الملاحظة، بالطبع، ما هي إلّا صياغة أخرى للحقيقة التي تنص على أن علاقة التكافؤ ـ الترافق ـ تفرق G إلى فصول تكافؤ منفصلة هي فصول الترافق. من الأهمية العظمى إيجاد قيمة c_a. ومن أجل عمل ذلك نسترجع مفهوما قدمناه في المسألة (١٣) بند (٢ ـ ٥) ولما كان هذا المفهوم مهم جدا ـ وهو من الأهمية بمكان بحيث إننا لا نترك الأمر لاحتمال حل المسألة من قبل الطالب ـ لذا فإننا نستعرض الآن ما قد يكون مألوفا للعديد من القراء.

تعريف

إذا كان $a\in G$ فإن $N(a)$ منظم (Normalizer) a في G، هو المجموعة $N(a)=\{x\in G|xa=ax\}$.

إن $N(a)$ يتكون تماما من تلك العناصر في G التي تتبادل مع a.

تمهيدية (٢-١١-٢)

$N(a)$ زمرة جزئية من G.

البرهان

إن رتبة G من حيث كونها منتهية أو غير منتهية ليست بذات أهمية في هذه النتيجة، لذلك فإننا لن نضع أي قيود على رتبة G.

لنفرض أن $x,y\in N(a)$ عندئذ $xa=ax$ و $ya=ay$ وبالتالي $(xy)a=x(ya)=(xa)y=(ax)y=a(xy)$ وهذا يقتضي أن $xy\in N(a)$ كما ينتج من كون $xa=ax$ أن $x^{-1}a=x^{-1}(ax)x^{-1}=x^{-1}(xa)x^{-1}=ax^{-1}$ لذلك فإن $x^{-1}\in N(a)$ ولكن هذا يثبت أن $N(a)$ زمرة جزئية من G.

إننا الآن في وضع يسمح لنا بعرض مبدأ العد.

مبرهنة (٢-١١-١)

إذا كانت G زمرة منتهية فإن $c_a=\dfrac{o(G)}{o(N(a))}$ وبعبارة أخرى، إن عدد العناصر المرافقة للعنصر a هو دليل منظم a في G.

البرهان

أولا: إن فصل الترافق للعنصر a في G ، $C(a)$ يتكون من جميع العناصر من الصيغة $x^{-1}ax$ لكل x في G. إن c_a يحسب عدد العناصر المختلفة من الصيغة $x^{-1}ax$.

إن طريقتنا في البرهان تتلخص في إثبات أن عنصرين في نفس المجموعة المشاركة اليمنى للزمرة الجزئية $N(a)$ يعطيان نفس المرافق للعنصر a بينما يعطى عنصران من مجموعتين مشاركتين يمنيين ومختلفتين للزمرة الجزئية $N(a)$ في G مرافقين مختلفين للعنصر a وبهذه الطريقة يكون لدينا تقابل بين مجموعة العناصر المرافقة للعنصر a والمجموعات المشاركة اليمنى للزمرة الجزئية $N(a)$.

لنفرض أن العنصرين x و y في G ينتميان إلى نفس المجموعة المشاركة اليمنى للزمرة الجزئية $N(a)$ في G ، عندئذ $y=nx$ حيث $n\in N(a)$ وبالتالي $na=an$. وحيث إن $y^{-1}=(nx)^{-1}=x^{-1}n^{-1}$ ، لذا فإن $y^{-1}ay=x^{-1}n^{-1}anx=x^{-1}ax$ أي أن x و y ينتجان نفس الفصل المرافق للعنصر a في G.

ومن ناحية أخرى، إذا كان x و y ينتميان إلى مجموعتين مشاركتين يمنيين مختلفتين للزمرة الجزئية $N(a)$ في G فإننا ندعي أن $x^{-1}ax\neq y^{-1}ay$ فإذا لم تكن هذه هي الحالة فإننا نستنتج من العلاقة $x^{-1}ax=y^{-1}ay$ أن $yx^{-1}a=ayx^{-1}$ الأمر الذي يقتضي أنّ $yx^{-1}\in N(a)$ والذي بدوره يقتضي أن x و y ينتميان إلى نفس المجموعة المشاركة اليمنى للزمرة الجزئية $N(a)$ في G ولكن هذا يناقض افتراضنا بأن x و y ينتميان إلى مجموعتين مشاركتين يمنيين مختلفتين وبهذا ينتهي البرهان.

نتيجة

$$o(G)=\Sigma\frac{o(G)}{o(N(a))}$$

حيث يتم الجمع على عنصر a من كل فصل ترافق.

البرهان

حيث إن $o(G)=\Sigma c_a$ ، لذا فإنه وفْقا للمبرهنة يتم برهان النتيجة.

إن المعادلة في النتيجة السابقة يطلق عليها عادة **معادلة الفصول** (Class equation) للزمرة G.

الآن نفحص هذه المفاهيم من أجل زمرة معينة وذلك قبل المضي إلى تطبيقات هذه النتائج. إنه لا داعي للنظر إلى الزمر الإبدالية وذلك لأن كل عنصرين يكونان مترافقين إذا وفقط إذا كانا متساويين (بمعنى أن $c_a=1$ لكل a) ولهذا نعود إلى مثالنا المألوف، الزمرة S_3 ، التي عناصرها e,(1,2),(1,3),(2,3),(1,2,3),(1,3,2). إن فصول الترافق هي كما يلي:

$c(e)=\{e\}$

$c(1,2)=\{(1,2),(1,3)^{-1}(1,2)(1,3),(2,3)^{-1}(1,2)(2,3),$

$(1,2,3)^{-1}(1,2)(1,2,3),(1,3,2)^{-1}(1,2)(1,3,2)\}$

(تحقق من ذلك) $=\{(1,2),(1,3),(2,3)\}$

(تحقق من ذلك أيضا) $c(1,2,3)=\{(1,2,3),(1,3,2)\}$

إن على الطالب التحقق من أن $N(1,2)=\{e,(1,2)\}$ وأن $N(1,2,3)=\{e,(1,2,3),(1,3,2)\}$

وبناء عليه فإن $c_{(1,2)}=\frac{6}{2}=3$ و $c_{(1,2,3)}=\frac{6}{3}=2$.

تطبيقات على مبرهنة (٢-١١-١)

إن للمبرهنة (٢-١١-١) تطبيقاً مباشراً وقوياً كما أننا لن نحتاج إلى توضيح استعمالاتها ذلك لأن النتائج الآتية التي توضح قوة المبرهنة هي نفسها مبرهنات لها مكانتها وأهميتها.

دعنا نعيد إلى الذاكرة تعريف مركز الزمرة، أي $Z(G)$ بأنه مجموعة كل العناصر $a\in G$ بحيث يكون $ax=xa$ لكل $x\in G$.

تمهيدية جزئية

$a\in Z$ إذا وفقط إذا كان $N(a)=G$ وإذا كانت G منتهية فإن $a\in Z$ إذا وفقط إذا كان $o(N(a))=o(G)$.

البرهان

إذا كان $a\in Z$ فإن $xa=ax$ لكل $x\in G$ ومن ثم فإن $N(a)=G$. وبالعكس، إذا كان $N(a)=G$ فإن $xa=ax$ لكل $x\in G$ وبالتالي فإن $a\in Z$. إذا كانت G منتهية فإن كون $o(N(a))=o(G)$ مكافىء لكون $N(a)=G$.

التطبيق الأول

مبرهنة (٢-١١-٢)

إذا كانت $o(G)=p^n$ ، حيث p عدد أولي فإن $Z(G)\neq(e)$.

البرهان

إذا كان $a\in G$ فإنه لكون $N(a)$ زمرة جزئية ولكون رتبة $N(a)$ قاسما لـرتبة G التـي تســاوي p^n لـذا فـإن رتـبــة $N(a)$ ، أي $o(N(a))$ ، يجـب أن تكـون مـن الـصيغـة $o(N(a))=p^{n_a}$. وكـذلك $a\in Z(G)$ إذا وفقط إذا كان $n_a=n$. بكتابة معادلة الفصول للزمرة G وبوضع $z=o(Z(G))$ نحصل على $p^n=o(G)=\Sigma\left(\frac{p^n}{p^{n_a}}\right)$.

ومع ذلك، وحيث إنه يوجد عناصر عددها z محققة للشرط $n_a=n$ فإننا نجد أن

$$p^n=z+\sum_{n_a<n}\left(\frac{p^n}{p^{n_a}}\right)$$

بالنظر إلى هذه المعادلة نجد أن العدد p قاسم للطرف الأيسر. ولما كان $n_a<n$ وذلك في كل حد من المجموع في الطرف الأيمن، لذا فإن

$$p\left|\frac{p^n}{p^{n_a}}=p^{n-n_a}\right.$$

وبناءً عليه فإن p قاسم لكل حد من هذا المجموع ومن ثم فإنه قاسم للمجموع كله وبالتالي

$$p\left|\left(p^n-\Sigma\left(\frac{p^n}{p^{n_a}}\right)\right)=z\right.$$

ولما كان $e\in Z(G)$ و $z\neq 0$ ، لذا فإن z عدد صحيح موجب يقبل القسمة على العدد الأولي p. وعليه فإن $z>1$ وهذا يدل على وجود عنصر خلاف e ينتمي إلى $Z(G)$ وهذا هو محتوى المبرهنة. إنه يمكن صياغة المبرهنة على النحو التالي: *«إن الزمرة التي رتبتها قوة لعدد أولي يجب أن يكون مركزها غير تافه»*.

الآن يمكن وبسهولة البرهان على نتيجة وردت سابقا في إحدى المسائل كنتيجة لهذه.

نتيجة

إذا كان $o(G)=p^2$ حيث p عدد أولي فإن G إبدالية .

البرهان

إن هدفنا هو إثبات أن $Z(G)=G$ ، على أية حال لقد أثبتنا أن $Z(G)\neq(e)$ هي زمرة جزئية من G لذلك فإن رتبة $Z(G)$ تساوي p أو p^2. فإذا كان $o(Z(G))=p^2$ فإن $Z(G)=G$ وبذلك نكون قد انتهينا من البرهان. لذلك نفرض أن $o(Z(G))=p$ وأن $a\in G$ و $a\notin Z(G)$. عندئذ $N(a)$ زمرة جزئية من G و $Z(G)\subset N(a)$ كما أن $a\in N(a)$. ولهذا فإن $o(N(a))>p$ ولكن استنادا إلى مبرهنة لاجرانج $o(N(a))|o(G)=p^2$. والمخرج الوحيد لهذه الحالة هو أن يكون $o(N(a))=p^2$ الأمر الذي يقتضي أن $a\in Z(G)$ وهذا مناقض للفرض بأن $a\notin Z(G)$. وبناء عليه فإن كون $o(Z(G))=p$ أمر لا يمكن تحقيقه، ومن ثم فإن $Z(G)=G$.

التطبيق الثاني

سنستخدم الآن مبرهنة (٢-١١-١) لإثبات مبرهنة مهمة جدا تنسب إلى العالم الرياضي كوشي ويمكن للقارىء أن يتذكر أن هذه المبرهنة قد أثبتت في حالة الزمر الإبدالية كتطبيق على النتائج التي توصلنا إليها في بند التشاكلات. وفي الحقيقة سنستخدم هذه الحالة، أي حالة الزمر الإبدالية، في برهان الحالة العامة. لكننا، بصراحة، سنثبت في البند القادم نتيجة أقوى من ذلك بكثير وهي التي تنسب إلى الرياضي سيلو والتي تكون مبرهنة كوشي نتيجة مباشرة لها وذلك باتباع طريقة تتجنب تماما مبرهنة (٢-١١-١) . وفي الواقع إنه لو كانت مبرهنة كوشي هي غايتنا الأساسية فإن بإمكاننا برهانها بالاستعانة بالمبادىء الأولية للزمر وذلك خلال سطور قليلة . (يجب أن ينظر القارىء إلى البرهان الجميل لمبرهنة كوشي المنسوب إلى مك - كي (McKay) والمنشور في مجلة :

American Mathematical monthly, **66** (1959), p.119.

وعلى أية حال فإننا نعرض هنا مبرهنة كوشي كتطبيق رائع لمبرهنة (٢-١١-١) .

مبرهنة (٢-١١-٣) كوشي

إذا كان p عددا أوليا وكان $p|o(G)$ فإن G تحوي عنصرا رتبته p.

البرهان

إننا نبحث عن عنصر $a\neq e$ في G بحيث يكون $a^p=e$. ولكي نثبت وجود هذا العنصر نستخدم الاستقراء الرياضي على $o(G)$ ، أي أننا نفرض صحة المبرهنة لجميع الـزمر T التي يكون من أجلها $o(T)<o(G)$. إنه لا يوجد أي داع للقلق حول البدء بالاستقراء لأن النتيجة صحيحة تماما لجميع الزمر التي رتبتها تساوي الواحد الصحيح .

إذا حدث وإن كانت W زمـرة جزئية من G و $W\neq G$ وكـان $p|o(W)$ فإنه وفقا لفرضية الاستقراء يوجد عنصر رتبته p في W ، ومن باب أولى فإنه يوجد هذا العنصر في G. لذلك فإن بإمكاننا أن نفرض أن p ليس قاسما لرتبة أية زمرة جزئية فعلية من G.

وبصورة خاصة، إذا كان $a\notin Z(G)$. وحيث إن $N(a)\neq G$ فإن $p\nmid o(N(a))$.

لنكتب الآن معادلة الفصول

$$o(G)=o(Z(G))+\sum_{N(a)\neq G}\frac{o(G)}{o(N(a))}$$

لما كان $p|o(G)$ و $p\nmid o(N(a))$. لذا فإنه يكون لدينا

$$p\left|\frac{o(G)}{o(N(a))}\right.$$

ومن ثم فإن

$$p\left|\sum_{N(a)\neq G}\frac{o(G)}{o(N(a))}\right.$$

وحيث إن $p|o(G)$ لذا نستنتج أن

$$p\left|\left(o(G)-\sum_{N(a)\neq G}\frac{o(G)}{o(N(a))}\right)=o(Z(G))\right.$$

وهكذا فإن $Z(G)$ زمرة جزئية من G رتبتها تقبل القسمة على p.

ولكننا قد افترضنا أن p ليس قاسما لرتبة أية زمرة جزئية فعلية من G ولهذا فإنه لا يمكن أن تكون $Z(G)$ زمرة جزئية فعلية من G.

وبــذلـك يتبقى لدينـا الإمكـانية الـوحيدة التي لا مفـر من قبـولها وهي أن $Z(G)=G$ وعنـدئـذ تكون G إبدالية . والآن يمكن الاستعانة بالنتيجة المبرهنة للزمر الإبدالية لإكمال الاستقراء وهذا يثبت المبرهنة .

ونختـم هـذا البنـد بدراسـة علاقـة الـترافق لنـوع خـاص مـن الزمـر هي زمـر التناظـــر S_n.

إذا كان لدينا أي عدد صحيح n فإننا نقول إن المتتالية من الأعداد الصحيحة المـوجبـة $n_1,n_2,\ldots,n_r$ حيث $n_1\leqslant n_2\leqslant\ldots\leqslant n_r$ تكون **تجزئة** (Partition) للعدد n إذا كان $n=n_1+n_2+\ldots+n_r$ لنفرض أن $p(n)$ ترمز إلى عدد تجزيئات العدد n ولنعين $p(n)$ لقيم صغيرة للعدد n.

$p(1)=1$ لأن 1 هو التجزئة الوحيدة لنفسه .

$p(2)=2$ لأن $2=2$ و $2=1+1$.

$p(3)=3$ لأن $3=3$ و $3=1+2$ و $3=1+1+1$.

$p(4)=5$ لأن $4=4$ و $4=1+3$ و $4=1+1+2$ و $4=1+1+1+1$ و $4=2+2$.

كذلك فإن

$$p(5)=7,\ p(6)=11,\ p(61)=1,121,505$$

كما أنه يوجد مراجع رياضية كثيرة حول $p(n)$.

إننـا نحصـل على تجزئة للعدد n وذلك عندما نحلل تبديلا في S_n إلى حاصل ضرب دورات منفصلة لأنه إذا كانت أطوال الدورات التي تظهر في التحليل هي $n_1,n_2,\ldots n_r$ ، $n_1\leqslant n_2\leqslant\ldots\leqslant n_r$ فإن $n=n_1+n_2+\ldots+n_r$.

سنقـول إن للتبديـل $\sigma\in S_n$ تفريقا دوريا $\{n_1,n_2,\ldots,n_r\}$ وذلك إذا أمكن كتابته على هيئة حاصل ضرب دورات منفصلة أطوالها $n_1,n_2,\ldots,n_r$ ، $n_1\leqslant n_2\leqslant\ldots\leqslant n_r$.

وهكذا فإن التفريق الدوري للتبديل $\sigma\in S_9$ حيث

$$\sigma=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 5 & 6 & 4 & 7 & 9 & 8 \end{pmatrix}=(1)(2,3)(4,5,6)(7)(8,9)$$

هو $\{1,1,2,2,3\}$. لاحظ أن $9=3+2+2+1+1$.

ننتقل الآن إلى البرهان على أن أي تبديلين في S_n يكونان مترافقين إذا وفقط إذا كان لهما التفريق الدوري نفسه، وعندما يتم هذا فإننا نستنتج من ذلك أن عدد فصول الترافق في S_n هو $p(n)$.

لكي نصل إلى هذا الهدف نعرض قاعدة بسيطة لحساب مرافقات تبديل معطى. لنفرض أن $\sigma \in S_n$ وأن σ يأخذ i إلى j. كيف نحسب $\theta^{-1}\sigma\theta$ ؟ لنفرض أن θ يأخذ i إلى s و j إلى t عندئذ $\theta^{-1}\sigma\theta$ يأخذ s إلى t. بعبارة أخرى، لكي تحسب $\theta^{-1}\sigma\theta$ استبدل أي رمز في σ بصورته تحت تأثير θ. فمثلا لكي نحسب $\theta^{-1}\sigma\theta$ حيث $\theta=(1,2,3)(4,7)$ و $\sigma=(5,6,7)(3,4,2)$ نتبع ما يلي:

بما أن

$$\theta: 5 \to 5,\ 6 \to 6,\ 7 \to 4,\ 3 \to 1,\ 4 \to 7,\ 2 \to 3$$

فإنه يمكن الحصول على $\theta^{-1}\sigma\theta$ من σ بعد استبدال 5 بـ 5 و 6 بـ 6 و 7 بـ 4 و 3 بـ 1 و 4 بـ 7 و 2 بـ 3 وذلك في التبديل θ وبالتالي فإن:

$$\theta^{-1}\sigma\theta=(5,6,4)(1,7,3)$$

بهذا الخوارزم لحساب المرافقات يصبح واضحا أنه إذا كان هناك تبديلان لهما التفريق الدوري نفسه فإنهما مترافقان. ذلك أنه إذا كان

$$\sigma=(a_1,a_2,\ldots a_{n_1})(b_1,b_2,\ldots,b_{n_2})\ldots(x_1,x_2\ldots x_{n_r})$$

وكان

$$\tau=(\alpha_1,\alpha_2\ldots\alpha_{n_1})(\beta_1,\beta_2\ldots\beta_{n_1})\ldots(\chi_1,\chi_2,\ldots\chi_{n_r})$$

فإن $\tau=\theta^{-1}\sigma\theta$ حيث يمكن استخدام التبديل

$$\theta=\begin{pmatrix} a_1a_2\ldots a_{n_1}\ b_1\ldots b_{n_2}\ldots\ x_1\ldots x_{n_r} \\ \alpha_1\alpha_2\ldots\alpha_{n_1}\ \beta_1\ldots\beta_{n_2}\ldots\ \chi_1\ldots\chi_{n_r} \end{pmatrix}$$

وهكذا على سبيل المثال، فإن التبديلين $(1,2)(3,4,5)(6,7,8)$ و $(7,5)(1,3,6)(2,4,8)$ مترافقان وذلك باستخدام التبديل:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 1 & 3 & 6 & 2 & 4 & 8 \end{pmatrix}$$

الآن لقد أصبح واضحا أن للتبديلين المترافقين التفريق الدوري نفسه لأنه باستخدام القاعدة التي رأيناها لحساب المرافق، نستبدل كل عنصر في الدورة المعطاة بصورته تحت تأثير التبديل الذي بواسطته تم الترافق.

الآن نعيد كتابة نص النتيجة الواردة في المناقشة السابقة كما يلي.

تمهيدية (٢-١١-٣)

إن عدد فصول الترافق في S_n هو $p(n)$ ، حيث $p(n)$ هو عدد تجزيئات العدد n.

إننا نستطيع إيجاد جميع العناصر المتبادلة مع تبديل معطى بعد وجود الوصف الصريح لفصول الترافق في S_n. ولنوضح ذلك بالمثال الآتي: إذا كان لدينا التبديل $(1,2)\in S_n$ فما هي العناصر التي تتبادل معه؟

بالتأكيد إن كل تبديل يبقي كلا من 1 و 2 ثابتا يتبادل مع $(1,2)$ ويوجد عناصر عددها $(n-2)!$ من هذا النوع.

كذلك فإن $(1,2)$ يتبادل مع نفسه وبهذه الطريقة نحصل على $2(n-2)!$ عنصرا في الزمرة المولدة بالعنصر $(1,2)$ والتبديلات التي عددها $(n-2)!$ والتي تبقي كلا من 1 و 2 ثابتاً.

هل يوجد عناصر أخرى؟

إن عدد المناقلات في S_n هو $\frac{n(n-1)}{2}$ وهي جميعها مرافقات لـ $(1,2)$ وبالتالي فإن فصل الترافق للعنصر $(1,2)$ يحوي $\frac{n(n-1)}{2}$ عنصرا.

فإذا كانت رتبة منظِّم $(1,2)$ هي r فإنه استنادا إلى مبدأ العد

$$\frac{n(n-1)}{2}=\frac{o(S_n)}{r}=\frac{n!}{r}$$

وهكذا فإن $r=2(n-2)!$. أي أن رتبة منظِّم $(1,2)$ هي $2(n-2)!$.

ولكننا رأينا أن عدد العناصر التي تتبادل مع $(1,2)$ هو $2(n-2)!$ وعليه فإن العنصر العام الذي يتبادل مع $(1,2)$ هو من الصيغة $\sigma=(1,2)^i\tau$ حيث i يساوي صفرا أو 1 كما أن τ هو التبديل الذي يبقي كلا من 1 و 2 ثابتاً .

وفي مجال آخر، لنعتبر التبديل $(1,2,3,\ldots,n)\in S_n$. إننا ندعي أن هذا التبديل يتبادل فقط مع قواه. بالتأكيد إنه يتبادل مع جميع قواه التي تعطينا n عنصرا. الآن إن أية دورة طولها n هي بالتأكيد مترافقة مع $(1,2,\ldots,n)$. إن عدد الدورات التي من هذا النوع في S_n هو $(n-1)!$. فإذا كانت رتبة منظم $(1,2,\ldots,n)$ في S_n هي u. وحيث إن عدد مرافقات $(1,2,\ldots,n)$ في S_n هو $\frac{o(S_n)}{u}$ ويساوي $(n-1)!$. لذا فإن $u=\frac{n!}{(n-1)!}=n$ ، أي أن رتبة منظم $(1,2,\ldots,n)$ في S_n هي n. وبما أن قوى $(1,2,\ldots n)$ تعطينا n عنصرا، فإنه لا يوجد أي عناصر أخرى وبهذا نكون قد برهنا على المطلوب.

مسائل

١ - أوجد جميع فصول الترافق في S_3 ثم أوجد c_a لكل a ثم تحقق من معادلة الفصول.

٢ - أوجد جميع فصول الترافق في S_4 ثم أوجد c_a لكل a وتحقق من معادلة الفصول.

٣ - أوجد جميع فصول الترافق في زمرة الوحدات الرباعية (انظر مسألة ٢١ بند ٢ - ١٠) كذلك أوجد c_a لكل a وتحقق من معادلة الفصول.

٤ - أوجد جميع فصول الترافق في الزمرة الزوجية التي رتبتها $2n$ ثم أوجد c_a لكل a وتحقق من معادلة الفصل. (لاحظ كيف أن الجواب يعتمد على نوعية n).

٥ - (ا) أثبت أن عدد الدورات المختلفة التي طولها r هو $\frac{1}{r}\frac{n!}{(n-r)!}$.

(ب) أوجد باستخدام (ا) عدد مرافقات الدورة $(1,2,\ldots,r)$ التي طولها r في S_n

(جـ) برهن على أن أي تبديل $\sigma\in S_n$ يتبادل مع $(1,2,\ldots,r)$ هو من الصيغة $\sigma=(1,2,\ldots,r)^i\tau$ حيث $i=0,1,2,\ldots,r$ كما أن τ هو التبديل الذي يبقي جميع الأعداد $1,2,\ldots,r$ ثابتة.

٦ - (ا) أوجد عدد مرافقات $(1,2)(3,4)$ في S_n ، $n\geq 4$.

(ب) أوجد صيغة لجميع العناصر التي تتبادل مع $(1,2)(3,4)$ في S_n .

٧ - إذا كان p عددا أوليا. فأثبت أن عدد العناصر في S_p والتي تحقق العلاقة $x^p=e$ هو $(p-1)!+1$ حيث $x \in S_p$.

٨ - إذا كان يوجد في زمرة G عنصر a له مرافقان فقط، فأثبت أن G تحتوي على زمرة ناظمية N بحيث إن $G \neq N \neq (e)$.

٩ - (أ) أوجد عنصرين في A_5 ، الزمرة المتناوبة من الدرجة الخامسة، بحيث يكونان مترافقين في S_5 لكنهما غير مترافقين في A_5 .

(ب) أوجد جميع فصول الترافق في A_5 وعدد العناصر في كل فصل.

١٠- (أ) إذا كانت N زمرة جزئية ناظمية في G و $a \in N$ فأثبت أن كل مرافق للعنصر $a \in G$ هو في N .

(ب) أثبت أن $o(N)=\sum c_a$ حيث a عنصر ما في N .

(جـ) باستخدام الفقرة (ب) ونتيجة المسألة ٩ (ب) أثبت أنه لا يوجد في A_5 زمرة ناظمية N غير (e) , A_5 .

١١- بالاستعانة بمبرهنة (٢-١١-٢) أثبت أنه إذا كان $o(G)=p^n$ حيث p عدد أولي فإن G تحتوي على زمرة جزئية رتبتها p^α حيث $o \leq \alpha \leq n$

١٢- إذا كانت $o(G)=p^n$ ، p عددا أوليا، فأثبت أنه يوجد زمر جزئية N_i ، $i=0,1,2,..,r$ حيث r عدد ما بحيث يكون $G=N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_r=(e)$ حيث N_i زمرة جزئية ناظمية في N_{i-1} و N_{i-1}/N_i إبدالية.

١٣- إذا كانت $o(G)=p^n$ ، p عددا أوليا، وكانت H زمرة جزئية من G و $H \neq G$ فأثبت أنه يوجد عنصر $x \in G$ و $x \notin H$ بحيث يكون $x^{-1}Hx=H$.

١٤- برهن على أن أية زمرة جزئية رتبتها p^{n-1} في الزمرة G التي رتبتها p^n ، حيث p عدد أولي، هي زمرة ناظمية في G .

*١٥- إذا كانت $o(G)=p^n$ ، p عددا أوليا، وكانت $N \neq (e)$ هي زمرة جزئية ناظمية في G فأثبت أن $N \cap Z \neq (e)$ حيث Z مركز G .

١٦- إذا كانت G زمرة مركزها Z وكانت G/Z دورية فأثبت أن G يجب أن تكون إبدالية.

١٧- أثبت أن أية زمرة رتبتها 15 هي زمرة دورية.

١٨- برهن على أن الزمرة التي رتبتها 28 تحتوي على زمرة جزئية ناظمية رتبتها 7 .

١٩ـ أثبت أنـه إذا كانت G زمرة رتبتها 28 وتحتوي على زمرة جزئية ناظمية رتبتها 4 فإن G إبدالية .

(٢ ـ ١٢) مبرهنة سيلو

تفيد مبرهنة لاجرانج بأن رتبة الزمرة الجزئية في الزمرة المنتهية قاسم لرتبة تلك الزمرة. إن العكس عموماً غير صحيح . إنه يوجد مبرهنات قليلة جدًّا تؤكد وجود زمر جزئية ذات رتب معينة في زمر منتهية . إن المبرهنة الأساسية والمستخدمة على نطاق واسع هي تلك المبرهنة التقليدية المنسوبة إلى الرياضي النرويجي سيلو.

نقدم هنا ثلاثة براهين لمبرهنة سيلو هذه. **البرهان الأول** منها هو برهان ممتع وأولي في الوقت نفسه منسوب إلى فيلانت *(Wielandt)* حيث ظهر في المجلة العلمية :

Archiv der Matematik, Vol **10**, (1959), pp. 401-402

إن العنصرين الأســاسيين في برهــان فيلانت هما نظرية الأعــداد ونــظرية التركيبات، ولهذا البرهان ميزة أخرى إلى جانب جودته وبساطته، هي الحصول على الزمرة الجزئية التي نبحث عنها .

إن **البرهان الثاني** مبني على استخدام الاستقراء الرياضي ومعادلة الفصول . وهو أحد البراهين القياسية التقليدية ، كما أنه توظيف جيد لمجموعة الأفكار المطوّرة إلى هذا الحد في هذا الكتاب والتي نستفيد منها لاشتقاق هذه النتيجة الأساسية للعالم سيلو .

أما **البرهان الثالث** فإن له فلسفة مختلفة تمامًا حيث إن الفكرة الأساسية فيه هي إثبات أنه إذا كانت هناك زمرة أكبر من تلك التي ندرسها تحقق استنتاج مبرهنة سيلو فإن الزمرة التي ندرسها يجب أن تحقق الاستنتاج نفسه. إن هذا يفرض علينا إثبات مبرهنـة سيلو لنـوع خاص من الـزمـر هو زمـر التنـاظـر، وبالاستعانة بمبرهنة كيلي (مـبرهنـة ٢ ـ ٩ ـ ١) يكـون باستطاعتنا استنتاج مبرهنة سيلو لجميع الزمر المنتهية.

وبغض النظر عن هذا الأسلوب الغريب وهو برهان شيىء لزمرة كبيرة ثم ببرهان ذات الشيء للزمرة المعطاة فإن للبرهان الثالث ميزاته أيضا وهي باستغلال الأفكار المستخدمة فيه نستطيع وبسهولة اشتقاق ما يسمى بمبرهنتي سيلو الثانية والثالثة .

قد يتساءل القارىء ولماذا إيراد هذه البراهين الثلاثة للمبرهنة نفسها مع أنه من الواضح أن واحدًا منها يكفي؟

إن الجواب على ذلك بسيط هو أن مبرهنة سيلو من الأهمية بمكان بحيث إنها تستحق هذا الأسلوب المتعدد الطرق، أضف إلى ذلك الطبيعة المتباعدة تماما للبراهين الثلاثة وكذلك التطبيق الجيد الذي يعطيه كل واحد منها للمواضيع التي تعلمناها إن هذه التبريرات مقنعة (على الأقل بالنسبة للمؤلف) والآن تذكر نص مبرهنة سيلو ونبدأ ببرهان فيلانت.

مبرهنة (٢-١٢-١) سيلو:

إذا كان p عددًا أوليا وكـــان $p^{\alpha}|o(G)$ فإن G تحتـوي على زمـرة جزئية رتبتهـا p^{α}.

قبـل الدخول في البرهان الأول لمبرهنة سيلو نحيد قليلا إلى مناقشة في نظرية الأعداد ونظرية التركيبات. إنه يمكن بسهولة إثبات أن عدد طرق اختيار مجموعة جزئية مكونة من k عنصر في مجموعة مكونة من n عنصر هو:

$$\binom{n}{k}=\frac{n!}{k!(n-k)!}$$

فإذا كان $n=p^{\alpha}m$ حيث p عدد أولي وإذا كان $p^{r}|m$ ولكن $p^{r+1}\nmid m$ فلنعتبر

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{p^\alpha!\,(p^\alpha m-p^\alpha)!}$$

$$= \frac{p^\alpha m(p^\alpha m-1)\ldots(p^\alpha m-i)\ldots(p^\alpha m-p^\alpha+1)}{p^\alpha(p^\alpha-1)\ldots\ldots(p^\alpha-i)\ldots\ldots(p^\alpha-p^\alpha+1)}$$

إن السؤال المطروح هو: ما هي قوة p التي تقسم $\binom{p^\alpha m}{p^\alpha}$ ؟

بالنظر إلى هذا العدد بالصيغة التي كتبناه بها يمكن لأي منا أن يرى أنه باستثناء الحد m في البسط فإن قوة p التي تقسم $(p^\alpha m-i)$ هي نفسها التي تقسم $(p^\alpha-i)$ ومن ثم فإن جميع قوى p تختصر ما عدى تلك القوى التي تقسم m وهكذا فإن

$$p^{r} \mid \binom{p^\alpha m}{p^\alpha} \quad \text{ولكن} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$$

البرهان الأول للمبرهنة:

لتكن $\mathcal{M}$. هي مجموعة جميع المجموعات الجزئية في G التي تحوي p^α عنصرًا وعليه فإن $\mathcal{M}$. تحوي $\binom{p^\alpha m}{p^\alpha}$ عنصرًا. إذا كان لدينا $M_1, M_2 \in \mathcal{M}$ (M_1 مجموعة جزئية من G تحوي p^α عنصرًا وكذلك الحال بالنسبة لـ M_2) نقول إن $M_1 \sim M_2$ إذا وُجد عنصر $g \in G$ بحيث يكون $M_1 = M_2 g$. إن من السهل التحقق من أن هذه هي علاقة تكافؤ على $\mathcal{M}$. .

إننا ندعي وجود، على الأقل، فصل تكافؤ من العناصر في $\mathcal{M}$. بحيث تكون عدد العناصر في هذا الفصل ليس مضاعفًا للعدد p^{r+1} ذلك أنه إذا كان p^{r+1} قاسمًا لعدد العناصر في كل فصل تكافؤ فإن p^{r+1} سيكون قاسماً لعدد

العنـاصر في $\mathcal{M}$. ولما كانت $\mathcal{M}$ تحوي $\binom{p^\alpha m}{p^\alpha}$ عنصرًا و $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$ فإن هذه لا يمكـن أن تكـون هي الحـالـة. ليكـن $\{M_1, ..., M_n\}$ فصـل تكـافـؤ في $\mathcal{M}$. حيث $p^{r+1} \nmid n$. من تعـريفـنـا للتـكـافـؤ في $\mathcal{M}$. إذا كان $g \in G$ فإنـه لكـل $i = 1,2,..,n$ يكـون $M_i g = M_j$ لقيمـة ما للعـدد j ، $1 \leqslant j \leqslant n$. لتكن $H = \{g \in G \mid M_1 g = M_1\}$ من الـواضـح أن H زمـرة جزئية من G لأنـه إذا كان $M_1 a = M_1$ و $M_1 b = M_1$ ومن ثم فإن $M_1 ab = (M_1 a) b = M_1 b = M_1$.

ستكون مهمتنا الآن إيجاد رتبة H . إننا ندعي أن $n\, o(H) = o(G)$ ونترك برهان ذلك للقارىء ولكننا نقترح عليه أن يستخدم المناقشة الواردة في مبدأ العد وذلك في بند (٢ ـ ١١).

الآن $no(H) = o(G) = p^\alpha m$ ولما كان $p^{r+1} \nmid n$ و $p^{\alpha+r} \mid p^\alpha m = no(H)$. لذلك فإنه يجب أن ينتج أن $p^\alpha \mid o(H)$ ومن ثم فإن $o(H) \geqslant p^\alpha$. بالإضافة إلى ذلك، إذا كان $m_1 \in M_1$ فإنـه لكـل $h \in H$ يكـون $m_1 h \in M_1$ وهـكـذا فإن M_1 تحوي على الأقـل $o(H)$ عنصرًا مختلفا. ولكن M_1 مجموعة جزئية من G تحوي p^α عنصرًا وهـكـذا نجـد أن $o(H) \leqslant p^\alpha$ وبـالجمـع ما بين هذه النتيجـة مع كون $o(H) \geqslant p^\alpha$ نحصـل على $o(H) = p^\alpha$. بهذا نكـون قد حصلنـا على زمـرة جزئية من G تحوي تماما p^α عنصرًا ألا وهي H. وهذا يثبت المبرهنة. إن هذا في الواقع قد أثبت أكثر من ذلك إذ أنه قد كوَّن الزمرة الجزئية المطلوبة.

إن ما عرف عادة بمبرهنة سيلو ليس إلاَّ حالة خاصة من مبرهنة (٢ ـ ١٢ ـ ١) ألا وهي:

نتيجة

إذا كان $p^m \mid o(G)$ و $p^{m+1} \nmid o(G)$ فإن G تحتوي على زمرة جزئية رتبتها p^m .

إن الزمرة الجزئية من G التي رتبتها p^m حيث $p^m \mid o(G)$ ولكن $p^{m+1} \nmid o(G)$ تدعى **زمرة سيلو الجزئية من نوع** *p* (*p*-Sylow subgroup) .

إن النتيجة السابقة تؤكد أن أية زمرة منتهية تحتوي على زمرة سيلو الجزئية من نوع *p* وذلك لكل عدد أولي *p* يقسم رتبتها. وبالطبع فإن مرافقة زمرة سيلو من نوع *p* هي زمرة سيلو من نوع *p* أيضا. بعد قليل سنرى كيف أن زمرتي سيلو الجزئيتين من نوع *p* في G بالنسبة للعدد الأولي *p* نفسه مرتبطتان ببعضهما وسنحصل على بعض المعلومات حول عدد زمر سيلو الجزئية من نوع *p* في G بالنسبة للعدد الأولي *p* . لكن قبل الانتقال إلى هذا نريد إعطاء برهانين آخرين لمبرهنة سيلو. وقبل البدء في البرهان الثاني نود إيراد الملاحظة الآتية التي رأيناها قبل النتيجة أعلاه مباشرة وهي أن تلك النتيجة حالة خاصة من المبرهنة. ورغم ذلك، فإننا ندعي أنه يمكن اشتقاق المبرهنة بسهولة من النتيجة، أي أنه إذا علمنا أن G تحتوي على زمرة جزئية رتبتها p^m حيث $p^m \mid o(G)$ ولكن $p^{m+1} \nmid o(G)$ فإننا نعلم أن G تحتوي على زمرة جزئية رتبتها p^α وذلك لأي عدد α بحيث يكون $p^\alpha \mid o(G)$. إن هذا ينتج من مسألة ١١ بند (٢ ـ ١١) التي تنص على أن أية زمرة رتبتها p^m ، حيث *p* عدد أولي، تحتوي على زمرة جزئية رتبتها p^α لأي عدد α ، $0 \leqslant \alpha \leqslant m$. وكما سنشرع مرة أخرى، في إثبات مبرهنة (٢ ـ ١٢ ـ ١) وبطريقتين مختلفتين يكفي أن نبرهن على وجود زمرة سيلو الجزئية من نوع *p* في G لكل عدد أولي *p* يقسم رتبة G .

البرهان الثاني لمبرهنة سيلو

سنبرهن بالاستقراء الرياضي على رتبة G أن G تحتوي على زمرة سيلو الجزئية من نوع *p* وذلك لكل عدد أولي *p* يقسم رتبة G .

إذا كانت $o(G) = 2$ فإن العدد الأولي المناسب هو 2 والزمرة G تحتوي، بالتأكيد، على زمرة جزئية رتبتها 2 هي G نفسها.

لذلك نفرض أن المبرهنة صحيحة لكل الزمر التي رتبتها تقل عن رتبة G ومن هذا نثبت أن المبرهنة سارية المفعول بالنسبة للزمرة G .

لذلك نفرض أن $p^m \mid o(G)$ وأن $p^{m+1} \nmid o(G)$ ، حيث p عدد أولي، $m \geq 1$.
فإذا كان $p^m \mid o(H)$ حيث H هي أية زمـرة جزئية من G ، $H \neq G$ فإنـه من فرضية الاستقراء نجد أن H تحتوي على زمرة جزئية T رتبتها p^m ، لما كانت T زمرة جزئية من H وH زمـرة جزئية من G فإن T زمرة جزئية من G ، عندئذ تكون T هي الزمرة الجزئية المطلوبة والتي رتبتها p^m .

لذلك يمكن أن نفرض أن $p^m \nmid o(H)$ ، **لأية** زمرة جزئية H من G ، $H \neq G$ وهنا نقصر اهتمامنا على مجموعة محدودة من هذه الزمر الجزئية. نعيد إلى الذاكرة أنه إذا كان $a \in G$ فإن $N(a) = \{x \in G \mid xa = ax\}$ زمرة جزئية من G ، وفضلا عن ذلك، إذا كان $a \notin Z$ ، حيث Z هو مركز G فإن $N(a) \neq G$ ، كذلك نعيد إلى الذاكرة أن معادلة الفصول للزمرة G تنص على أن

$$o(G) = \sum \frac{o(G)}{o(N(a))}$$

حيث يتم الجمع على عنصر واحد من كل فصل ترافق. وبفصل هذا المجموع إلى حدين أولهما تلك العناصر التي تنتمي إلى المركز وثانيهما تلك العناصر التي لا تنتمي إليه نجد أن

$$o(G) = z + \sum_{a \notin Z} \frac{o(G)}{(oN(a))}$$

حيث $z = o(Z)$

الآن نستعين بالتخصيص الذي أوردناه وهو أن $p^m \nmid o(H)$ لأية زمرة جزئية H من G بحيث $H \neq G$ وذلك يجعل $H = N(a)$ حيث $a \notin Z$ ولما كان في هذه الحالة $P^m \mid o(G)$ و $p^{m+1} \nmid o(N(a))$ لذا فإنه يجب أن يكون لدينا

$$P \mid \frac{o(G)}{o(N(a))}$$

وبكتابة هذه النتيجة أي،

$$P \mid \frac{o(G)}{o(N(a))}$$

مرة أخرى لكل $a \in G$ ، $a \notin Z$. ومن معادلة الفصول، والمعلومات التي بين أيدينا من ضمنها أن $p^m \mid o(G)$ فإنه لابد أن يكون $p \mid o(G)$ كذلك نجد أن

$$p \mid \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

وهكذا نجد من معادلة الفصول أن $p|z$. الآن بما أن $p|z=o(Z)$ واستنادا إلى مبرهنة كوشي (مبرهنة ٢ ـ ١١ ـ ٣) نجد أن Z تحوي عنصراً $b \neq e$ رتبته p . لتكن $B = (b)$ هي الزمرة الجزئية من G المولدة بالعنصر b . إن رتبة B هي p . وفضلا عن ذلك بما أن $b \in Z$ فإن B يجب أن تكون ناظمية في G ولذلك نستطيع تكوين الزمرة الخارجة $\bar{G} = G/B$. وبالنظر إلى $\bar{G}$ ، نجد **أولاً** أن رتبتها هي

$$\frac{o(G)}{o(B)} = \frac{o(G)}{p}$$

وبالتالي فإن رتبتها تقل عن $o(G)$ ، **ثانيا**، إن $p^{m-1} \mid o(\bar{G})$ ، ولكن $P^m \nmid o(\bar{G})$ ومن فرضية الاستقراء نجد أن $\bar{G}$ تحتوي على زمرة جزئية $\bar{P}$ رتبتها p^{m-1} . لتكن $P=\{x \in G \mid xB \in \bar{P}\}$. إن P هي زمرة جزئية من G وفقا لتمهيدية (٢ ـ ٧ ـ ٥) وزيادة على ذلك $\bar{P} \approx P/_B$ (برهن ذلك). وهكذا فإن

$$p^{m-1} = o(\bar{P}) = \frac{o(P)}{o(B)} = \frac{o(P)}{P}$$

وبالتالي فإن $o(P) = p^m$. وبناءًا عليه فإن P هي زمرة سيلو الجزئية من نوع p المطلوبة. وبهذا ينتهي الاستقراء ومن ثم ينتهي البرهان.

بهذا نكون قد انتهينا من البرهان الثاني لمبرهنة سيلو. لاحظ أنه يمكن تكييف البرهان الثاني بسهولة لإثبات أنه إذا كان $p \mid o(G)$ فإن G تحتوي على زمرة جزئية رتبتها p^{α} مباشرة دون الاستعانة ببرهان وجود زمرة سيلو الجزئية من نوع P (إن هذه هي المسألة الأولى من المسائل الواردة في نهاية هذا البند).

الآن ننتقل إلى البرهان الثالث لمبرهنة سيلو.

البرهان الثالث لمبرهنة سيلو

قبل المُضي قُدماً في تفاصيل البرهان، يجدر بنا أن نلخص الخطة الأساسية سنثبت **أولاً** أن جميع زمر التناظر S_{p^r}، حيث p عدد أولي تحتوي على زمر سيلو الجزئية من نوع p . وستكون **الخطوة الثانية** هي إثبات أنه إذا كانت G محتواة في M وكانت M تحتوي على زمرة سيلو الجزئية من نوع p فإن G تحتوي على زمرة سيلو الجزئية من نوع p . **وأخيراً** سنثبت بالاستعانة بمبرهنة كيلي أننا نستطيع استخدام S_{p^k}، حيث k عدد كبير بشكل كاف، لتكون هي M . وبهذا تكون لدينا جميع أجزاء البرهان وينتهي بذلك إثبات المبرهنة.

لتنفيذ هذا البرنامج بالتفصيل، يجب علينا معرفة درجة كِبَر زمرة سيلو الجزئية من نوع p في S_{p^r} . إن هذا سيجعل من الضروري معرفة قوى p التي تقسم $(p^r)!$. إن هذا سيكون سهلا بيد أن الحصول على زمرة سيلو الجزئية من نوع p في S_{p^r} . سيكون أصعب.

لتنفيذ خطوة أخرى أساسية في هذا المخطط المبدئي سيكون من الضروري تقديم علاقة تكافؤ جديدة في الزمر بحيث تكون فصول التكافؤ المقابلة لهذه العلاقة هي تلك المجموعات المعروفة **بالمجموعات المشاركة المزدوجة** وسيكون لهذا فوائد عديدة ليست فقط في مواصلة برهان مبرهنة سيلو فحسب بل في حصولنا أيضا على الجزئين الثاني والثالث من مبرهنة سيلو الشاملة.

الآن نبدأ بمهمتنا الأولى وهي إيجاد قوى العدد الأولي p التي تقسم ! (p^k) . وفي الواقع فإن من السهل إيجاد ذلك من أجل ! n لأي عدد صحيح n (أنظر مسألة ٢) . ولكنه سيكون واضحا وكافيا أن نوجد ذلك فقط من أجل ! (p^k) .

لنعرف n(k) بأنه ذلك العدد الذي يكون من أجله ! $p^{n(k)} \mid (p^k)$ ولكن ! $p^{n(k)+1} \nmid (p^k)$.

تمهيدية (٢ ـ ١٢ ـ ١)

$$n(k)= 1+p+\ldots+p^{k-1}$$

البرهان

إذا كان k=1 ، ونظرا لأن $p! = 1\times2\times\ldots(p-1).p$ فإن من الواضح أن $p \mid p!$ ولكن $p^2 \nmid p!$ لذلك فإن n(1)=1 كما هو مطلوب .

ما هي الحدود في مفكوك ! (p^k) التي يمكن أن تسهم في قوى p والتي تقسم ! (p^k) ؟

من الواضح أنها فقط مضاعفات p أي $p, 2p, \ldots, p^{k-1}p$ وبعبارة أخرى n(k) يجب أن يكون قوة للعدد p التي تقسم

$$p(2p)(3p)\ldots(p^{k-1}p)= p^{p^{k-1}}(p^{k-1})!\ .$$

ولكن ، عندئذ ، $n(k)= p^{k-1}+n(k-1)$ ،
وبالمثل $n(k-1)=n(k-2)+p^{k-2}$ وهكذا . . . وبكتابة هذه المقادير على الصيغة :

$$nk-n(k-1) = p^{k-1}$$

$$n(k-1)-n(k-2) = p^{k-2}$$

$$\vdots$$

$$n(2)-n(1) = p$$

$$n(1) = 1$$

ثم الجمع نحصل في النهاية على:

$$n(k) = 1+p + p^2 + \dots + p^{k-1}$$

وهذا هو المطلوب إثباته وبذلك ينتهي برهان التمهيدية.

نحن الآن على استعداد لإثبات أن S_{p^k} تحتوي على زمرة سيلو الجزئية من نوع p، أي سنعرض (بل، في الواقع سنحصل على) زمرة جزئية رتبتها $p^{n(k)}$ في S_{p^k}.

تمهيدية (٢ - ١٢ - ٢):

إن S_{p^k}. تحتوي على زمرة سيلو الجزئية من نوع p.

البرهان:

بالاستقراء على k. إذا كان $k=1$ فإن رتبة العنصر $(12\dots p)$ في S_p هي p. ولذلك فإن هذا العنصر يولد زمرة جزئية رتبتها p. ولما كان $n(1)=1$ لذا فإن النتيجة صحيحة عندما $k=1$.

لنفرض أن النتيجة صحيحة من أجل $k-1$ ونثبت صحتها من أجل k.

لنقسم الأعداد الصحيحة $1,2,\dots,p^k$ إلى مجموعات عددها p بحيث تحتوي كل مجموعة على p^{k-1} عنصرًا وذلك كما يلي:

$$\{1,2,\dots,p^{k-1}\},\{p^{k-1}+1,p^{k-1}+2,\dots,2p^{k-1}\},\dots,\{(p-1)p^{k-1}+1,\dots,p^k)$$

إن التبديل σ المعرف كما يلي:

$$\sigma=(1,p^{k-1}+1,2p^{k-1}+1,\dots,(p-1)p^{k-1}+1)\dots(j,p^{k-1}+j,2p^{k-1}+j,\dots,(p-1)p^{k-1}+1+j)$$
$$\dots(p^{k-1},2p^{k-1},\dots,(p-1)p^{k-1},p^k)$$

يتمتع بالخواص الآتية:

(١) $\sigma^p = e$

(٢) إذا كان τ هو التبديل الذي يبقى كل i ثابتا، حيث $i>p^{k-1}$. (ولذلك فهو يؤثر فقط على $1,2,\dots,p^{k-1}$) فإن $\sigma^{-1}\tau\sigma$ يحرك فقط عناصر في المجموعة $\{p^{k-1}+1, p^{k-1}+2, \dots, 2p^{k-1}\}$.

وبـــصـــورة عامـــة، فإن $\sigma^{-i}\tau\sigma^{i}$ يحرك فقط عنـــاصر في المـــجـــمـــوعـــة $\{jp^{k-1}+1, jp^{k-1}+2, \ldots, (j+1)p^{k-1}\}$ لنعتبر $\tau(i)=i\}$ إذا كان $A = \{\tau \in S_{p^k} | i > p^{k-1}$.

إن A زمـرة جزئية من S_{p^k} ، كما أن عنــاصر A تستطيع إجراء أي تبديل على العناصر $1, 2, \ldots, p^{k-1}$ ومن هنا ينتج بسهولة أن $A \approx S_{p^{k-1}}$ واستنادًا إلى فرضية الاستقراء فإن A تحتوي على زمرة جزئية P_1 رتبتها $p^{n(k-1)}$.

لتكن
$T = P_1(\sigma^{-1}P_1\sigma)(\sigma^{-2}\ P_1\sigma^2) \ldots\ldots (\sigma^{-(P-1)}P_1\sigma^{P-1}) = P_1P_2 \ldots\ldots P_{n-1}$ حيث $P_i = \sigma^{-i}P_1\sigma^{i}$.
إن P_i متـماثلة مع P_1 لكل i ولهذا فإن رتبة P_i هي $p^{n(k-1)}$ كما أن الـــعـــنـــاصر في P_i المختلفة تؤثر على المجموعات غير المتداخلة من الأعداد الصحيحة ولذلك فإن هذه العناصر **تتبادل مع بعضها** وهكذا فإن T زمرة جزئية من S_{p^k} .

ما هي رتبة T ؟ لما كان $P_i \cap P_j = (e)$ وذلك عندما $0 \leqslant i \neq j \leqslant p-1$ لذلك نجد أن $o(T) = o(P_1)^p = p^{pn(k-1)}$. إننا لم نحصل، بعد، على ما نريد تماما ذلك لأن T ليست هي زمرة سيلو الجزئية من نوع p التي نحن بصدد البحث عنها.

لما كان $\sigma^p = e$ و$\sigma^{-i}P_1\sigma^{i} = P^i$ فإنه يكون لدينا $\sigma^{-1}T\sigma = T$ لنكن

$$P = \{\sigma^j t \,|\, t \in T,\ o \leqslant j \leqslant p-1\}$$

لما كان $\sigma \notin T$ و$\sigma^{-1}T\sigma = T$ فإنه يكون لدينا أمران، أولهما هو أن T زمرة جزئية من S_{p^k} وثانيهما هو أن $o(P) = p.o(T) = p\ p^{n(k-1)p} = p^{n(k-1)p+1}$.

أخيرًا لقد وجدنا ضالتنا، حيث إن P هي زمرة سيلو الجزئية من نوع p والتي كنا نبحث عنها في S_{p^k} . لنجد السبب. حسنًا، إن رتـبـتـهـــا هـــي $p^{n(k-1)p+1}$ ولكن $n(k-1) = 1+p+\ldots+p^{k-2}$ ، لذلك، $pn(k-1)+1 = 1+p+\ldots.+p^{k-1} = n(k)$ ، ولما كان $o(P) = p^{n(k)}$ لذا فإن P هي، بالفعل، زمرة سيلو الجزئية من نوع p في S_{p^k} .

ملاحظة حول البرهان

إن هذا البرهان لا يثبت التمهيدية فقط بل إنه في الواقع يسمح لنا بتكوين زمر سيلو الجزئية من نوع p استقرائيا. ونتبع طريقة البرهان لتكوين زمر سيلو الجزئية من نوع 2 في S_4 .

لنقسم 1,2,3,4 إلى مجموعتين هما {1,2} ، {3,4} ولتكن $P_1=((1,2))$ و $\sigma=(1\ 3)(2\ 4)$ عندئذ $P_2=\sigma^{-1}P_1\sigma=((3,4))$.

وعليه فإن زمـرة سيلو الجزئية من نوع 2 هي الزمرة المولدة بالتبديل $(1,3)\ (2,4)$ وT ، حيث

$$T = P_1P_2 = \{(1,2), (3,4), (1,2)\ (3,4), e\}$$

لكي ننفذ برنامج البرهان الثالث الذي أوجزناه سابقا نقدم الآن علاقة تكافؤ جديدة في الزمر (أنظر مسألة **٣٩** بند **٢-٥**).

تعريـف

لتكن G زمرة ، A وB زمرتين جزئيتين من G . إذا كان $x,y\in G$ فلنعرف أن $x\sim y$ إذا كان $y=axb$ حيث $a\in A$ ، $b\in B$.

نترك للقارىء برهان التمهيدية الآتية نظرًا لسهولتها .

تمهيدية (٢ - ١٢ - ٣)

إن العلاقة المعرفة آنفا هي علاقة تكافؤ على G كما أن فصل تكافؤ العنصر $x\in G$ هو المجموعة $AxB = \{axb \mid a\in A, b\in B\}$

يطلق على المجموعة AxB **المجموعة المشاركة المزدوجة** للزمرتين الجزئيتين A وB في G .

إذا كانت كل من A وB زمـرتـين جزئيتـين منتهيتين في G فما هو عدد عناصر المجموعة المشاركة المزدوجة؟

أولا: إن التطبيق T ، حيث، $T:A\varkappa B \to A\varkappa B\varkappa^{-1}$ والمعرف بالقاعدة $(a\varkappa b)T = a\varkappa b\varkappa^{-1}$ هو تطبيق أحادي وغامر (تحقق من ذلك) وبالتالي فإن $o(A\varkappa B) = o(A\varkappa B\varkappa^{-1})$

ولما كانت $\varkappa B\varkappa^{-1}$ زمرة جزئية من G رتبتها هي نفس رتبة B ووفقا لمبرهنة (٢ ـ ٥ ـ ١) نجد أن:

$$o(A\varkappa B) = o(A\varkappa B\varkappa^{-1}) = \frac{o(A)o(\varkappa B\varkappa^{-1})}{o(A\cap\varkappa B\varkappa^{-1})} = \frac{o(A)\,o(B)}{o(A\cap\varkappa B\varkappa^{-1})}$$

بهذا نكون قد أثبتنا التمهيدية الآتية:

تمهيدية (٢ ـ ١٢ ـ ٤)

إذا كانت A وB زمرتين جزئيتين منتهيتين من G فإن:

$$o(A\varkappa B) = \frac{o(A)o(B)}{o(A\cap \varkappa B\varkappa^{-1})}$$

الآن نأتي إلى الخطوة المهمة من البرهان الثالث لمبرهنة سيلو.

تمهيدية (٢ ـ ١٢ ـ ٥)

لتكن G زمرة منتهية ولنفرض أن G هي زمرة جزئية من الزمرة المنتهية M ولنفرض، أيضا، أن M تحتوي على زمرة سيلو الجزئية Q من نوع p . عندئذ G تحتوي على زمرة سيلو الجزئية P من نوع p . في الحقيقة، $P=G\cap\varkappa Q\varkappa^{-1}$ ، $\varkappa\in M$.

البرهان

يجدر بنا قبل البدء في البرهان بالتفصيل أن نوضح الفرضية أكثر قليلا.

لنفرض أن $p^m|o(M)$ وأن $p^{m+1}\nmid o(M)$ وأن Q زمرة جزئية من M رتبتها p^m ولنفرض أن $o(G) = p^n t$ حيث $p\nmid t$ ونريد الحصول على زمرة جزئية P من G رتبتها p^m .

لنعتبر تفريق M إلى المجموعات المشاركة المزدوجة للزمرتين الجزئيتين G و Q أي أن $M = \cup GxQ$. ومن تمهيدية (٢ ـ ١٢ ـ ٤) نجد أن :

$$o(GxQ) = \frac{o(G)o(Q)}{o(G\cap xQx^{-1})} = \frac{p^n t\, p^m}{o(G\cap xQx^{-1})}$$

ولما كانت $G\cap xQx^{-1}$ زمرة جزئية من xQx^{-1} ، لذا فإن رتبتها هي p^{m_x} . نحن ندعي أن $m_x = n$ وذلك لعنصر ما $x\in M$ ، فإذا لم يكن الأمر كذلك، فإن

$$o(GxQ) = \frac{p^n t p^m}{p^{m_x}} = t\,p^{\,m+n-m_x}$$

ولذلك فإنه يقبل القسمة على p^{m+1} . ولما كانت $M = \cup\, GxQ$ وحيث إن هذا إتحـاد منفصـل، لذا فإن $o(M) = \sum o(GxQ)$ حيث يتم الجمـع على عنصر من كل مجموعة مشاركة مزدوجة. ولكن $p^{m+1} \mid o(GxQ)$ لذلك فإن $p^{m+1} \mid o(M)$ ولكن هذا يناقض كون $p^{m+1} \nmid o(M)$ ولهذا نجد أن $m_x = n$ لعنصر ما $x\in M$ ، وعندئذ $o(G\cap xQx^{-1}) = p^n$. وحيث إن $G\cap xQx^{-1}$ زمرة جزئية من G رتبتها p^n ، لذا فإن برهان التمهيدية يكون قد انتهى.

الآن نستطيع، وبسهولة، إثبات مبرهنة سيلو. وفقا لمبرهنة كيلي (مبرهنة ٢ـ٩ـ١) فإننا نستطيع إدخال الزمرة المنتهية G تماثليا في زمرة التناظر S_n من الدرجة n .

لنختار k بحيث يكون $n<p^k$. عندئذ نستطيع إدخال S_n تماثليا في S_{p^k} (وذلك بالتأثير على الأعداد $1,2,\ldots,n$ في المجموعة $1,2,\ldots,n,\ldots,p^k$) لذا فإن G مدخلة تماثليا في S_{p^k} . واستنادًا إلى تمهيدية (٢ـ١٢ـ٢) نجد أن S_{p^k} تحتوي على زمرة سيلو الجزئية من نوع p واستنـادًا، كذلك، إلى تمهيدية (٢ـ١٢ـ٥) فإن G يجب أن تحتوي على زمرة سيلو الجزئية من نوع p . وبذلك ينتهي البرهان الثالث لمبرهنة سيلو.

لقد أمدنا البرهان الثالث بأكثر مما نريد ألاَ وهو أننا نستطيع الحصول منه على الجزئين الآخرين من مبرهنة سيلو.

مبرهنة (٢-١٢-٢) (الجزء الثاني من مبرهنة سيلو)

إذا كانت G زمرة منتهية وكان $p^n \mid o(G)$ ولكن $p^{n+1} \nmid o(G)$، حيث p عدد أولي فإن أي زمرتين جزئيتين من G رتبتاهما هي p^n مترافقتان.

البرهان

لتكن A وB زمرتين جزئيتين من G ، $o(A) = o(B) = p^n$ ونريد إثبات أن $A = gBg^{-1}$ لعنصر ما g من G .

الآن نفرق G إلى المجموعات المشاركة المزدوجة لـ A و B ، أي $G = \cup AxB$.

استنادًا إلى تمهيدية (٢-١٢-٤) يكون لدينا

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

فإذا كانت $A \neq xBx^{-1}$ لكل $x \in G$ فإن $o(A \cap xBx^{-1}) = p^m$ حيث $m<n$.

وبالتالي فإن :

$$o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{2n-m} \qquad ,2n-m \geqslant n+1$$

ولما كان $p^{n+1} \mid o(AxB)$ لكل x ، وحيث إن $o(G) = \sum o(AxB)$ لذا فإننا نحصل على تناقض وهو أن $p^{n+1} \mid o(G)$ ، لذلك فإن $A = gBg^{-1}$ لعنصر ما $g \in G$. وهذا هو ما تضمنته المبرهنة.

إن معرفتنا بأنه لعدد أولي p تكون جميع زمر سيلو الجزئية من نوع p مترافقة يتيح لنا أن نحسب وبدقة عدد هذه الزمر الجزئية من G . إن السبيل إلى ذلك هو نفسه الذي ورد في إثبات مبرهنة (٢-١١-١) .

لقد ناقشنا في مسائل سابقة (أنظر مثلا مسألة ١٦ بند ٢ـ٥) منظِّم الزمرة الجزئية H المعرف كما يلي $N(H) = \{x \in G \mid xHx^{-1} = H\}$ ، عنـدئـذ، كما في برهان مبرهنة (٢ـ١١ـ١) نجد أن *عدد المرافقات المختلفة لـ H ، أي xHx^{-1} ، في G هو دليل $N(H)$ في G* ولما كانت جميع زمر سيلو الجزئية من نوع p مترافقة فإنه يكون لدينا:

تمهيدية (٢ـ١٢ـ٦)

إن عدد زمـر سيلو الجـزئية من نوع p يساوي $\dfrac{o(G)}{o(N(P))}$ حيث P هي إحدى زمر سيلو الجزئية من نوع p وبصورة خاصة إن هذا العدد قاسم لرتبة G .

ومع ذلك يستطيع الواحد منا أن يقول الشيء الكثير حول عدد زمر سيلو الجزئية من نوع p ، لعدد أولي ما p . وهذا ما سنناقشه الآن كما أن الطريقة ستتضمن استخدام المجموعات المشاركة المزدوجة.

مبرهنة ٢ـ١٢ـ٣ (الجزء الثالث من مبرهنة سيلو)

إن عدد زمـــر سيلو الجـــزئـية من نوع p ، حيث p عدد أولي، في G هو من الصيغة $1 + kp$.

البرهان

لتكن P هي زمـرة سيلو الجزئية من نوع p في G . ولنفرق G إلى المجموعات المشـاركـة المـزدوجـة لـP وP وهكـذا $G = \cup PxP$. الآن ما هو عدد عنـاصر PxP ؟ من تمهيدية (٢ـ١٢ـ٤) نعلم أن الجواب هو:

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}$$

فإذا كان $P \cap xPx^{-1} \neq P$ فإن $p^{n+1} \mid o(PxP)$ ، حيث $p^n = o(P)$. وبـعـبـــارة أخـــرى، إذا كان $x \notin N(P)$ فإن $p^{n+1} \mid o(PxP)$. أيضـــا إذا كان $x \in N(P)$ فإن $PxP = P(Px) = P^2x = Px$ ، لذلك فإنه في هذه الحالة يكون $o(PxP) = p^n$.

الآن

$$o(G) = \sum_{x\in N(P)} o(PxP) + \sum_{x\notin N(P)} o(PxP)$$

حيث يتم كل مجموع على عنصر من كل مجموعة مشاركة مزدوجة، لاحظ أن PxP=Px وذلك عندما x∈N(P) ، وبناءً عليه فإن المجموع الأول يصبح $\sum_{x\in N(P)} o(Px)$ وذلك على المجموعات المشاركة المختلفة للزمرة الجزئية P في N(P) وبالتالي فإن المجموع الأول يكون o(N(P)) . ماذا يمكن أن نقول عن المجموع الثاني؟ لقد رأينا أن كل حد من الحدود المكونة له قابل للقسمة على p^{n+1} ولذلك فإن

$$p^{n+1} \mid \sum_{x\notin N(P)} o(PxP)$$

وهكذا فباستطاعتنا كتابة المجموع الثاني على الصيغة

$$\sum_{x\notin N(P)} o(PxP) = p^{n+1}u$$

ولذلك فإن

$$o(G) = o(N(P)) + p^{n+1}u$$

وبالتالي فإن

$$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}$$

لاحظ أن: o(N(P))|o(G) لأن N(P) زمرة جزئية من G ، كذلك $\frac{p^{n+1}u}{o(N(P))}$ عدد صحيح ولما كان $p^{n+1} \nmid o(G)$ ، لذا فإن $p^{n+1} \nmid o(N(P))$ ولكن عندئذ، $\frac{p^{n+1}u}{o(N(P))}$ **يجب أن يقبل القسمة على** p ولذلك يمكن كتابة $\frac{p^{n+1}u}{o(N(P))}$ على الصيغة kp ، حيث k عدد صحيح . وبالتعويض في المعادلة الواردة أعلاه يكون لدينا:

$$\frac{o(G)}{o(N(P))} = 1 + kp$$

وحيث إن $\frac{o(G)}{o(N(P))}$ هو عدد زمر سيلو الجزئية من نوع p في G ، لهذا فإننا بذلك نكون قد أنهينا إثبات المبرهنة.

في المسائل (٢٠ ـ ٢٤) من المسائل الإضافية في نهاية هذا الفصل، يوجد موجز لأسلوب آخر لبرهان الجزئين الثاني والثالث من مبرهنة سيلو.

ونختتم هذا البند بتوضيح لكيفية استخدام أجزاء مبرهنة سيلو وذلك من أجل الحصول على معلومات كثيرة عن الزمر المنتهية.

لتكن G هي الزمرة التي رتبتها $11^2.13^2$. نريد تعيين عدد زمر سيلو الجزئية من نوع 11 في G وكذلك الحال بالنسبة لعدد زمر سيلو الجزئية من نوع 13 .

إن عدد زمر سيلو الجزئية من نوع 11 هو 1+11k وذلك وفقا لمبرهنة (٢ ـ ١٢ ـ ٣) وأيضا وفقا لتمهيدية (٢ ـ ١٢ ـ ٥) فإن هذا العدد يجب أن يقسم $11^2.13^2$ وحيث إن 1+11k أولي بالنسبة للعدد 11 لذلك فإنه يجب أن يقسم 13^2 . **هل يوجد عامل للعدد 13^2 من الصيغة 1+11k ؟**

من الواضح أنه لا يمكن أن يوجد له عامل غير العدد 1 نفسه وهكذا فإن 1=1+11k وبالتالي فإن عدد زمر سيلو الجزئية من نوع 11 في G يجب أن يكون زمرة واحدة. ولما كانت جميع زمر سيلو الجزئية من نوع 11 مترافقة (مبرهنة ٢ـ١٢ـ٢) لذلك نستنتج أن زمرة سيلو الجزئية من نوع 11 ناظمية في G . ماذا يمكن أن نقول عن زمر سيلو الجزئية من نوع 13 ؟ إن عددها هو من الصيغة 1+13k ويجب أن يقسم

$11^2.13^2$ ومن ثم فإنه يجب أن يقسم 11^2 وهنا، أيضا، نستنتج أن عدد زمر سيلو الجزئية من نوع 13 هو زمرة واحدة ويجب أن تكون ناظمية في G .

الآن نعلم أن G تحتوي على زمرتين جزئيتين ناظميتين هما B, A ورتبتاهما $13^2, 11^2$ على الترتيب. ومن نتيجة مبرهنة (٢-١١-٢) فإن أية زمرة رتبتها p^2 هي زمرة إبدالية، حيث p عدد أولي. وبالتالي فإن B,A إبداليتان. ولما كان $A\cap B=(e)$ فإننا نجد بسهولة أن $G=AB$.

أخيرا إذا كان $a\in A$ و $b\in B$ فإن $aba^{-1}b^{-1}= a(ba^{-1}b^{-1})\in A$ وذلك لأن A ناظمية كذلك فإن $aba^{-1}b^{-1} =(aba^{-1})b^{-1}\in B$ لأن B ناظمية وبالتالي فإن $aba^{-1}b^{-1}\in A\cap B=(e)$ وهذا يقتضي أن $aba^{-1}b^{-1}=e$ وبالتالي فإن $ab=ba$ حيث $b\in B,a\in A$. إن هذا مع كون $G=AB$ ، A و B إبداليتين يسمح لنا أن نستنتج أن G إبدالية. وبناءً عليه فإن أية زمرة رتبتها $11^2.13^2$ يجب أن تكون إبدالية.

الآن نورد توضيحًا آخر لاستخدام أجزاء مبرهنة سيلو المختلفة. لتكن G هي الزمرة التي رتبتها 72 . إذن $o(G)= 2^3 3^2$. **كم عدد زمر سيلو الجزئية من نوع 3 في G ؟**

لنفرض أن هذا العدد هو t ، عندئذ من مبرهنة (٢-١٢-٣) نجد أن t هو من الصيغة $t=1+3k$. وأيضا وفقا لتمهيدية (٢-١٢-٥) فإن $t|72$ وبما أن t أولي بالنسبة للعدد 3 لذلك فإنه يجب أن يكون لدينا $t|8$. إن العوامل الوحيدة للعدد 8 من الصيغة $1+3k$ هي 1 و 4 ولذا فإن $t=1$ أو $t=4$ هما الاحتمالان الوحيدان. وبعبارة أخرى، إن عدد زمر سيلو الجزئية من نوع 3 هو إما زمرة واحدة أو 4 زمر جزئية.

فإذا كان عدد زمر سيلو الجزئية من نوع 3 هو زمرة واحدة فقط وحيث إن جميع زمر سيلو الجزئية من نوع 3 مترافقة فإن زمرة سيلو الجزئية من نوع 3 يجب أن تكون

ناظمية في G وفي هذه الحالة تحتوي G ، بالتأكيد، على زمرة جزئية ناظمية غير تافهة. ومن ناحية أخرى، إذا كان عدد زمر سيلو الجزئية من نوع 3 في G هو 4 فإنه وفقا لتمهيدية (٢-١٢-٥) يكون دليل N في G هو 4 حيث N هو مُنظِّم زمرة سيلو الجزئية من نوع 3 . ولكن $72 \nmid 4!=i(N)!$ ووفقا لتمهيدية (٢-٩-١) يجب أن تحتوي N على زمرة جزئية ناظمية غير تافهة في G (رتبتها على الأقل هي 3) وهكذا، مرة أخرى، نستطيع أن نستنتج أن G تحتوي على زمرة جزئية ناظمية غير تافهة. وخلاصة القول، أن أية زمرة رتبتها 72 يجب أن تحتوي على زمرة جزئية ناظمية غير تافهة ولهذا فإنها لا يمكن أن تكون زمرة بسيطة.

مسائل

١ - كيِّف البرهان الثاني لمبرهنة سيلو لتثبت مباشرة أنه إذا كان p عددًا أوليا وكان $p^\alpha | o(G)$ ، فإن G تحتوي على زمرة جزئية رتبتها p^α .

٢ - إذا كان $x>0$ عددًا حقيقيا فإننا نعرف $[x]$ بأنه العدد الصحيح m بحيث يكون $m \leq x < m+1$ فإذا كان p عددًا أوليا. فأثبت أن قوى p التي تقسم $n!$ تعطى بالآتي:

$$[\frac{n}{p}]+[\frac{n}{p^2}]+\ldots+[\frac{n}{p^r}]+\ldots$$

٣ - استخدم طريقة تكوين زمرة سيلو الجزئية من نوع p في S_{p^k} لإيجاد مولدات الزمرتين الآتيتين:

(ا) زمرة سيلو الجزئية من نوع 2 في S_8 .

(ب) زمرة سيلو الجزئية من نوع 3 في S_9 .

٤ - استعمل الطريقة المستخدمة في مسألة ٣ لإيجاد مولدات الزمرتين الآتيتين:

(ا) زمرة سيلو الجزئية من نوع 2 في S_6 .

(ب) زمرة سيلو الجزئية من نوع 3 في S_6 .

٥ - إذا كان p عددًا أوليا فأوجد صيغة مولدات زمرة سيلو الجزئية من نوع p في S_{p^2} .

٦ - ناقش عدد وطبيعة زمر سيلو الجزئية من نوع 3 ومن نوع 5 في الزمرة التي رتبتها $3^2.5^2$.

٧ - لتكن G هي الزمرة التي رتبتها 30

(ا) أثبت أن زمرة سيلو الجزئية من نوع 3 أو من نوع 5 في G يجب أن تكون ناظمية .

(ب) من الفقرة (ا) أثبت أن أية زمرة من زمر سيلو الجزئية من نوع 3 ومن نوع 5 في G يجب أن تكون ناظمية في G .

(جـ) أثبت أن G تحتوي على زمرة جزئية ناظمية رتبتها 15 .

(د) باستخدام الفقرة (جـ) صنف جميع الزمر التي رتبها 30 .

(هـ) كم عدد الزمر غير المتماثلة والمختلفة التي رتبها 30 .

٨ - إذا كانت G زمـرة رتبتها 231 فأثبت أن زمرة سيلو الجزئية من نوع 11 محتواة في مركز G .

٩ - إذا كانت G زمـرة رتبتهـا 385 فأثبت أن زمـرة سيلو الجزئية من نوع 11 ناظمية في G كما أن زمرة سيلو الجزئية من نوع 7 محتواة في مركز G .

١٠ - إذا كانت G زمـــرة رتبتهـا 108 فأثبت أن G تحتـوي على زمـرة جزئية ناظمية رتبتها 3^k حيث $k\geqslant 2$.

١١ - إذا كانت $o(G) = pq$ ، حيث p ، q عددان أوليان مختلفان $p<q$ فأثبت ما يلي :

(ا) إذا كان $p\nmid (q-1)$ فإن G دورية .

(ب)* إذا كان $p|(q-1)$ فإنه يوجد زمرة غير إبدالية وحيدة رتبتها pq .

١٢* - لتكن G هي الزمرة التي رتبتها pqr ، حيث p ، q ، r أعداد أولية و $p<q<r$.
أثبت ما يلي :

(ا) إن زمرة سيلو الجزئية من نوع r ناظمية في G .

(ب) إن G تحتوي على زمرة ناظمية رتبتها qr .

(جـ) إذا كان $q\nmid (r-1)$ فإن زمـــرة سيلو الجـــزئـــية من نوع q في G هي ناظمية في G .

١٣ - إذا كانت G زمرة رتبتها p^2q ، حيث إن p ، q عددان أوليان فأثبت أن G تحتوي على زمرة جزئية ناظمية غير تافهة .

١٤ - إذا كانت رتبة G تساوي p^2q ، حيث p ، q عددان أوليان فأثبت أن زمرة سيلو الجزئية من نوع p أو زمرة سيلو الجزئية من نوع q في G يجب أن تكون ناظمية في G .

١٥ - لتكن G زمرة منتهية بحيث يكون لكل b,a في G $(ab)^p=a^pb^p$ حيث p عدد أولي يقسم رتبة G . أثبت أن

(ا) زمرة سيلو الجزئية من نوع p في G ناظمية في G .

(ب)* إذا كانت P هي زمرة سيلو الجزئية من نوع p في G فإنه يوجد زمرة جزئية ناظمية N في G بحيث إن $P\cap N=(e)$ و $PN=G$.

(جـ) مركز الزمرة G غير تافه.

١٦** - إذا كانت G زمرة منتهية بحيث إن زمرة سيلو الجزئية P من نوع p محتواة في مركز G فأثبت أنه يوجد زمرة جزئية ناظمية N في G بحيث يكون $P\cap N=(e)$ و $PN=G$.

١٧* - إذا كانت H زمرة جزئية من G وكان $N(H)=\{x\in G \mid xHx^{-1}=H\}$ وإذا كانت P هي زمرة سيلو الجزئية من نوع p . فأثبت أن $N(N(P))=N(P)$.

١٨* - لتكن P هي زمرة سيلو الجزئية من نوع p في G وبفرض أن a,b عنصران من مركز P وأن $a=xbx^{-1}$ لعنصر ما x في G . أثبت أنه يوجد عنصر $y\in N(p)$ بحيث يكون $a=yby^{-1}$.

١٩** - لتكن G زمـرة منتهية، وليكن ϕ تماثلا ذاتيا على G بحيث إن ϕ^3 هو التماثل الذاتي المحايد. إفرض الآن أن $\phi(x)=x$ يقتضي أن يكون $x=e$. أثبت أن زمرة سيلو الجزئية من نوع p هي ناظمية في G وذلك لكل عدد أولي p قاسم لرتبة G .

*٢٠ - لتكن G هي زمـرة المصفوفات غير الشاذة من النوع $n\times n$ على مجموعة الأعداد الصحيحة قياس العدد الأولي p . أوجد زمرة سيلو الجزئية من نوع p .

٢١ - أوجد العدد الممكن لزمر سيلو الجزئية من نوع 11 ، من نوع 7 ومن نوع 5 الممكنة في الزمرة التي رتبتها $5^2.7.11$.

٢٢ - إذا كانت $G=S_3$ و $A=((1,2))$ زمـرة جزئية من G فأوجـد جميع المجمـوعـات المشاركة المزدوجة AxA للزمرة الجزئية A في G .

٢٣ - إذا كانت $G=S_4$ و $A=((1,2,3,4))$ و $B=((1,2))$ فأوجــد جميع المجمــوعـات المشاركة المزدوجة AxB للزمرتين الجزئيتين A و B في G .

٢٤ - إذا كانت G هي الـزمـرة الـزوجية التي رتبتهـا 18 والمولـدة بالعنصرين a و b بحيث إن $a^2=b^9=e$ و $ab=b^{-1}a$ فأوجد جميع المجموعات المشاركة المزدوجة للزمرتين الجزئيتين $H=(a)$ و $K=(b^3)$ في G .

(٢-١٣) الضرب المباشر

لقد احتجنا في مناسبات عديدة في هذا الفصل إلى إنشاء زمرة جديدة من بعض زمر معروفة لدينا، فعلى سبيل المثال لقد أنشأنا زمرة جديدة باستخدام زمرة معلومة وأحد تماثلاتها الذاتية وذلك في نهاية البند (٢ ـ ٨). أيضا لقد رأينا سابقا حالة خاصة من هذا النوع من الإنشاء في المثال المتكرر والمتعلق بالزمرة الزوجية.

ورغم ذلك، فإنه لم تحدث أية محاولة بعد لإيجاد وسيلة منظمة لبناء زمر جديدة من زمر معطاة. وسنفعل ذلك الآن. إن الطريقة التي سنتبعها هي أبسط طريقة مباشرة لتركيب الزمر للحصول على زمر أخرى.

نبدأ، **أولاً**، بزمرتين مع أنه ليس للعدد اثنين أية خصوصية. ومع ذلك، ومن الخبرة التي لدينا سنتمكن من معالجة الحالة لأي عدد منته من الزمر بسهولة وسرعة. وهنا نكرر أنه ليست لذلك العدد المنتهي من الزمر أية خصوصية. إننا نستطيع إعادة المناقشة وذلك على نطاق واسع لأي عدد من الزمر على حد سواء بيد أننا لسنا بحاجة إلى ذلك الوضع العام هنا ولذلك نحسم الأمر في حالة عدد منته من الزمر وذلك كهدف نهائي لنا.

لتكن A و B زمـرتـين، ولنعتـبر الضرب الديكارتي (الذي ناقشناه في الفصل الأول) $G=A\times B$ للزمـرتـين A و B . إن G تتكـون من جميع الأزواج المرتبة (a,b) حيث $a\in A$ و $b\in B$.

هل نستطيع توظيف العمليتين المعرفتين على A و B لتزويد G بضرب يجعل منها زمرة؟ لماذا لا نحاول الطريقة الواضحة وهي ضرب المركبات المتقابلة؟

دعنا نعرف حاصل ضرب (a_1,b_1) و (a_2,b_2) في G كما يلي:
$(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2)$. إن حاصل الضرب a_1a_2 في المركبة الأولى هو حاصل ضرب العنصرين a_2, a_1 في الزمرة A كما أن حاصل الضرب $b_1 b_2$ في المركبة الثانية هو حاصل ضرب العنصرين b_2, b_1 في الزمرة B . بهذا التعريف يكون لدينا، على الأقل، حاصل ضرب معرف على G .

هل يمكن أن تكون G زمرة بالنسبة لهذا الضرب؟

إن الجواب على ذلك نعم ومن السهل التحقق منه كما يلي: نبدأ بالتحقق من **قانون التجميع** ولتكن (a_1,b_1) و (a_2,b_2) و (a_3,b_3) ثلاثة عناصر من G عندئذ

$$((a_1,b_1)(a_2,b_2))(a_3,b_3) = (a_1a_2, b_1b_2)(a_3,b_3) = ((a_1a_2)a_3, (b_1b_2)b_3)$$

بينما

$$(a_1,b_1)((a_2,b_2)(a_3,b_3)) = (a_1,b_1)(a_2a_3, b_2b_3) = (a_1(a_2a_3), b_1(b_2b_3))$$

وحيث إن قانون التجميع محقق في كل من B, A لذا فإن هذا يثبت لنا أن الضرب المعرف على G هو، بالفعل، تجميعي.

نأتي الآن إلى **العنصر المحايد**. ليس غريباً أن نجرب العنصر (e,f) ليكون العنصر المحايد في G حيث e هو العنصر المحايد في f,A هو العنصر المحايد في B .

لدينا

$$(a,b)(e,f) = (ae,bf) = (a,b)$$

و

$$(e,f)(a,b) = (ea,fb) = (a,b)$$

أي أن (e,f) هو العنصر المحايد في G .

أخـيرا نريد **إيجـاد معـكـوس أي عنصر في** G . هنـا، أيضـا، لماذا لا نحاول العنصر (a^{-1}, b^{-1}) ليكون معكوس (a,b) ؟ الآن

$$(a^{-1},b^{-1})\,(a,b) = (a^{-1}a,b^{-1}b) = (e,f)$$

و

$$(a,b)\,(a^{-1},b^{-1}) = (aa^{-1},bb^{-1}) = (e,f)$$

وبالتالي فإن العنصر (a^{-1},b^{-1}) هو، بالفعل، معكوس العنصر (a,b) . بهذا نكون قد تحققنا من أن $G = A \times B$ هي زمرة. وندعو هذه الزمرة زمرة حاصل **الضرب المباشر الخارجي** (External Direct Product) للزمرتين A وB .

ولما كانت $G=A\times B$ قد بُنِيت من A وB بمثل هذه الطريقة البسيطة، فإننا نتوقع أن بنية كل من A وB سينعكس كليا على بنية G . وهذا هو ما حصل فعلا، فإن معرفة A وB تعطينا، تماما، معلومات كاملة حول بنية $A\times B$.

إن إنشاء $G=A\times B$ كان من الخارج ونريد الآن أن نعكس الوضع ونحاول إنشاء G من الداخل.

لنـعـتـبر: $\widetilde{A} = \{(a,f)\in G \mid a\in A\}\subset G = A\times B$ حيث f هو الـعـنصر المحايد في B . ماذا نتوقع من $\widetilde{A}$ ؟ والإجابة على ذلك هو أن $\widetilde{A}$ زمرة جزئية من G كما أن $\widetilde{A}\approx A$. لكي نثبت هذا التماثل، لنعرف $\phi:A\to\widetilde{A}$ ، بالقاعدة $\phi(a)=(a,f)$ حيث $a\in A$. إن من البسـاطة بمكان إثبات أن ϕ تماثل من A على $\widetilde{A}$ وأن $\widetilde{A}$ زمـرة جزئية من G . وفضـلا عن ذلـك فإن $\widetilde{A}$ ناظمية في G لأنـه إذا كان $(a_1,b_1)\in G,(a,f)\in\widetilde{A}$ فإن

$$(a_1,b_1)\,(a,f)\,(a_1,b_1)^{-1} = (a_1,b_1)\,(a,f)\,(a_1^{-1},b_1^{-1})$$
$$= (a_1aa_1^{-1},b_1fb_1^{-1}) = (a_1aa_1^{-1},f) \in \widetilde{A}$$

وبالتالي يكون لدينا صورة مماثلة للزمرة A في G هي $\tilde{A}$ والتي هي زمرة جزئية ناظمية في G .

إن ما عملناه بالنسبة إلى A يمكن عمله أيضا من أجل B . فإذا كانت $\tilde{B} = \{(e,b) \in G | b \in B\}$ فإن $\tilde{B}$ متماثلة مع B كما أنها زمرة جزئية ناظمية في G .

إننا ندعي أكثر من ذلك وهو أن $G = \tilde{A}\tilde{B}$ كما أن كل عنصر $g \in G$ يحلل بطريقة وحيدة على الصيغة $g = \bar{a}\bar{b}$ ، حيث $\bar{a} \in \bar{A}$, $\bar{b} \in \bar{B}$ لأنه إذا كان $g = (a,b) = (a,f)\ (e,b)$ ، وحيث إن $(a,f) \in \bar{A}$, $(e,b) \in \bar{B}$ فإننا نجد أن $g = \bar{a}\bar{b}$ ، هنا $\bar{a} = (a,f)$, $\bar{b} = (e,b)$. **لماذا يكون هذا التحليل وحيدا؟**

لأنه إذا كان $(a,b) = \bar{x}\,\bar{y}$ حيث $\bar{x} \in \bar{A}$, $\bar{y} \in \bar{B}$ فإن $\bar{x} = (x,f)$, $x \in A$, $\bar{y} = (e,y)$, $y \in B$ وهكذا فإن $(x,y) = (x,f)(e,y) = \bar{x}\,\bar{y}$ وبالتالي فإن $x = a$ و $y = b$ ولهذا فإن $\bar{x} = \bar{a}$, $\bar{y} = \bar{b}$.

وهكذا نكون قد تحققنا من أن G هي حاصل ضرب داخلي $\bar{A}\bar{B}$ لزمرتين جزئيتين ناظميتين هما $\tilde{A}$ التي تماثل A و $\bar{B}$ التي تماثل B بطريقة هي أن لكل عنصر $g \in G$ تمثيل وحيد على الصيغة $g = \bar{a}\bar{b}$ حيث $\bar{a} \in \bar{A}$, $\bar{b} \in \bar{B}$ ننتقل الآن إلى مناقشة حاصل ضرب زمر عددها n حيث $n > 1$ عدد صحيح .

لتكن $G_1, G_2, \ldots, G_n$ مجموعة من الزمر عددها n ولتكن :

$$G = G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) | g_i \in G_i\}$$

هي مجموعة جميع العديدات من رتبة n ، أي حاصل الضرب الديكارتي للزمر $G_1, G_2, .., G_n$. نعرف الضرب على G وفق ما يلي :

$$(g_1, g_2, \ldots, g_n)\ (g'_1, g'_2, \ldots, g'_n) = (g_1 g'_1, g_2 g'_2, \ldots, g_n g'_n)$$

وذلك بضرب المركبات المتقابلة ببعضها. إن حاصل الضرب في المركبة i قد تم إجراءه في الزمرة G_i . إن G زمرة عنصرها المحايد هو $(e_1,e_2,\dots,e_n)$ حيث e_i هو العنصر المحايد في الزمرة G_i كما أن $(g_1,g_2,\dots,g_n)^{-1}=(g_1^{-1},g_2^{-1},\dots,g_n^{-1})$ ندعو هذه الزمرة زمرة حاصل الضرب المباشر الخارجي للزمر $G_1,G_2,\dots,G_n$. لتكن

$$\widetilde{G}_i=\{(e_1,e_2,\dots,e_{i-1},g_i,e_{i+1},\dots,e_n)\mid g_i\in G_i\}$$

عنـدئـذ $\widetilde{G}_i$ زمـرة جزئـية ناظمية في G كما أن $\bar{G}_i\approx G_i$. وفضـلا عن ذلـك، $G=\bar{G}_1\bar{G}_2\dots\bar{G}_n$ كما يوجـد لكـل عنصر $g\in G$ تحليل وحـيد $g=\bar{g}_1\bar{g}_2\dots\bar{g}_n$ حيث $\hat{g}_1\in\tilde{G}_1,\dots,\hat{g}_n\in\tilde{G}_n$ ونترك التحقق من هذه الأمور للقارىء.

هنا، أيضا، كما في حالة $A\times B$ ، لقد حصلنا على الزمرة G كحاصل ضرب داخـلي لزمر جزئية ناظمية $\bar{G}_1,\bar{G}_2,\dots\bar{G}_n$ بحيث إن كل عنصر ممثل بطريقة وحيدة كحاصل ضرب العناصر $\bar{g}_1\dots\bar{g}_n$ حيث $\bar{g}_i\in\bar{G}_i$. وبالتالي نعطي التعريف الآتي:

تعريـف

*إذا كانت G زمرة، وكانت $N_1,N_2,\dots,N_n$ زمرًا جزئية **ناظمية** في G بحيث إن:*

(١) $G=N_1N_2\dots N_n$.

(٢) *كل عنصر $g\in G$ يمكن كتابته بطريقة وحيدة على الصيغة $g=m_1m_2\dots m_n$ ، $m_i\in N_i$. فعندئذ نقول إن G هي حاصل الضرب المباشر الداخلي (Internal Direct product) للزمر $N_1,N_2,\dots,N_n$*

قبل الاستمرار في الموضوع، دعنا نرى مثالا لزمرة هي عبارة عن حاصل الضرب المباشر الداخلي لبعض زمرها الجزئية.

لتكن G هي الزمرة الإبدالية المنتهية التي رتبتها $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ ، حيث $p_1,p_2,\dots,p_k$ أعداد أولية مختلفة و $\alpha_i>0$ لكل i . وإذا كانت $P_1,P_2,\dots,P_k$ هي زمر سيلو الجزئية من الأنواع $p_1,p_2,\dots,p_k$ على الترتيب في G ، فإن G هي حاصل الضرب المباشر الداخلي للزمر $P_1,P_2,\dots,P_k$ (أنظر مسألة ٥).

والآن نستأنف المناقشة العامة. لنفرض أن G هي حاصل الضرب المباشر الداخلي للزمر الجزئية الناظمية $N_1,...,N_n$. إن $N_1,...,N_n$ هي زمر بحد ذاتها - لنتغاضى، في الوقت الحاضر، عن كونها زمر جزئية ناظمية. بإمكاننا تكوين الزمرة $T = N_1 \times N_2 \times ... \times N_n$ التي هي حاصل الضرب المباشر الخارجي للرمز $N_1,...,N_n$ من المتوقع أن T ، G مرتبطين نوعا ما. في الواقع، إن هدفنا هو إثبات أن G متماثلة مع T. فإذا استطعنا برهان ذلك فإنه من الممكن استبعاد كلمة خارجي وداخلي من العبارتين حاصل الضرب المباشر الخارجي، حاصل الضرب المباشر الداخلي. بعد هذا كله فإن هاتين الزمرتين ستكونان نفس الزمرة إلى حد التماثل وبالتالي فإننا نتحدث فقط عن الضرب المباشر.

ونبدأ بالتمهيدية الآتية.

تمهيدية (٢-١٣-١)

لنفرض أن G هي حاصل الضرب المباشر الداخلي للزمر $N_1,...,N_n$ ، عندئذ إذا كان $i \neq j$ فإن $N_i \cap N_j = (e)$ وإذا كان $a \in N_i$ و $b \in N_j$ فإن $ab = ba$.

البرهان

لنفرض أن $x \in N_i \cap N_j$ ، عندئذ يمكن كتابة x على الصيغة

$$x = e_1 \ldots e_{i-1} x e_{i+1} \ldots e_j \ldots e_n$$

حيث $e_t = e$ وذلك باعتبار x عنصرًا من N_i . وبالمثل يمكن كتابة x على الصيغة

$$x = e_1 \ldots e_i \ldots e_{j-1} x e_{j+1} \ldots e_n$$

حيث $e_t = e$ وذلك باعتبار x عنصرًا من N_j. بيد أن لكل عنصر، وخاصة x ، تمثيل وحيد على الصيغة $m_1 m_2 \ldots m_n$ حيث $m_1 \in N_1,...,m_n \in N_n$ وحيث إن هذين التفريقين للعنصر x يجب أن يتطابقا، لذا فإنه يجب تساوي المركبة من N_i في كل من التفريقين، وبالتالي، فإن المركبة في التفريق الأول هي x وفي الثانية هي e وعليه فإن $x = e$ ، وهكذا فإن $N_i \cap N_j = (e)$ عندما $i \neq j$.

لنفرض الآن أن $b \in N_j$, $a \in N_i$ وأن $i \neq j$ ، عندئذ $aba^{-1} \in N_j$ لأن N_j ناظمية وبالتالي فإن $aba^{-1}b^{-1} \in N_j$. وبالمثل، لما كان $a^{-1} \in N_i$ فإن $ba^{-1}b^{-1} \in N_i$ ومن ثم فإن

$aba^{-1}b^{-1} \in N_i$. بيد أنه عندئذ يكون $aba^{-1}b^{-1} \in N_i \cap N_j = (e)$ وبالتالي فإن $aba^{-1}b^{-1} = e$ الأمر الذي يترتب عليه أن $ab=ba$.

تجدر الإشارة هنا إلى أنه إذا كانت $K_1,\ldots,K_n$ زمرًا جزئية ناظمية في G بحيث إن $G=K_1K_2\ldots K_n$ وإن $K_i \cap K_j = (e)$ عندما $i \neq j$ **فإنه ليس ضروريا** أن تكون G هي حاصل الضرب المباشر الداخلي للزمر $K_1,\ldots,K_n$ ، لذلك فإننا بحاجة إلى شرط إضافي (أنظر مسألتي ٨، ٩).

بإمكاننا الآن برهان التماثل المطلوب بين حاصل الضرب المباشر الداخلي وحاصل الضرب المباشر الخارجي الذي ذكرناه سابقا.

مبرهنة (٢-١٣-١)

لتكن G زمرة ولنفرض أن G هي حاصل الضرب المباشر الداخلي للزمر $N_1,\ldots,N_n$ ولتكن $T=N_1 \times N_2 \times \ldots \times N_n$ عندئذ فإن G تماثل T .

البرهان

لنعرف التطبيق $\psi: T \to G$ بالقاعدة

$$\psi((b_1,b_2,\ldots,b_n)) = b_1b_2\ldots b_n$$

حيث $b_i \in N_i$ ، $i=1,2,\ldots,n$. إننا ندعي أن ψ تماثل من T على G .

أولا ، إن ψ تطبيق غامر ذلك أنه لما كانت G هي حاصل الضرب المباشر الداخلي للزمر $N_1,\ldots,N_n$ فإن $x=a_1a_2\ldots a_n$ ، حيث $a_1 \in N_1,\ldots,a_n \in N_n$ وعندئذ فإن

$$\psi((a_1,a_2\ldots a_n)) = a_1\, a_2\ldots a_n = x$$

إن التطبيق ψ أحادي وذلك وفقا لوحدانية تمثيل كل عنصر كحاصل ضرب عناصر من $N_1,N_2,\ldots,N_n$ ، أي أنه إذا كان

$$\psi((a_1,a_2,\ldots,a_n)) = \psi((c_1,c_2,\ldots,c_n))$$

حيث $a_i \in N_i$, $c_i \in N_i$, $i=1,2,..,n$ فإنه وفقا لتعريف ψ نجد أن $a_1a_2...a_n=c_1c_2...c_n$ ولكن وفقا لشرط الوحدانية الوارد في تعريف حاصل الضرب المباشر الداخلي ينتج أن: $a_1=c_1,\ldots, a_n=c_n$ ، أي أن ψ أحادي.

كل ما بقي لدينا هو إثبات أن ψ تشاكل من T على G . فإذا كان $X, Y \in T$ حيث $X=(a_1,\ldots,a_n)$ و $Y=(b_1,\ldots,b_n)$ فإن:

$$\psi(XY) = \psi((a_1,\ldots,a_n)(b_1,\ldots,b_n)) = \psi(a_1b_1, a_2b_2,\ldots,a_nb_n)$$
$$= a_1b_1a_2b_2\ldots\ldots a_nb_n$$

واستنادا إلى تمهيدية (٢-١٣-١) فإن $a_ib_j=b_ja_i$ عندما $i\neq j$ وبالتالي فإن

$$a_1b_1a_2b_2\ldots a_nb_n=a_1a_2\ldots a_n\, b_1b_2\ldots b_n$$

وهكذا فإن

$$\psi(XY)=a_1a_2\ldots a_nb_1b_2\ldots b_n$$

لكن،

$$\psi(Y) = \psi(b_1,b_2,\ldots,b_n) = b_1b_2\ldots b_n,\ \psi(X) = \psi((a_1,a_2,\ldots,a_n)) = a_1a_2\ldots a_n$$

ولذلك فإن $\psi(XY) = \psi(X)\psi(Y)$ مما ينهي البرهان.

لاحظ أمرًا معيناً تثبته المبرهنة أعلاه أنه إذا كانت زمرة G تماثل حاصل الضرب المباشر الخارجي لزمر معينة G_i فإن G ، في الواقع، هي حاصل الضرب المباشر الداخلي للزمر $\bar{G}_i$ التي تماثل G_i ونقول، ببساطة، إن G هي حاصل الضرب المباشر للزمر $\bar{G}_i$ (أو G_i).

سنرى في البند القادم أن كل زمرة إبدالية منتهية هي عبارة عن حاصل ضرب مباشر لزمر دورية. وعندما يكون هذا لدينا سنكون ملمين تماماً ببنية جميع الزمر الإبدالية المنتهية.

وتجدر الإشارة هنا إلى أن ما يشبه حاصل الضرب المباشر للزمر موجود في دراسة جميع البنى الجبرية وسنرى هذا فيما بعد عند دراسة فضاءات المتجهات والحلقات والفضاءات الحلقية. إن المبرهنات التي تصف بنية جبرية بدلالة حاصل الضرب المباشر لبنى جبرية من النوع نفسه لكنها أبسط وصفا (وعلى سبيل المثال كما في حالة الزمر الإبدالية) لهي مبرهنات مهمة بصورة عامة. من خلال مثل هذه المبرهنات نستطيع اختزال بنى جبرية معقدة إلى دراسة بنى أسهل منها.

مسائل

١ - إذا كانت B,A زمرتين فأثبت أن $A\times B\approx B\times A$

٢ - إذا كانت G_1, G_2, G_3 ثلاث زمر فأثبت أن $(G_1\times G_2)\times G_3 \approx G_1\times G_2\times G_3$. حاول تعميم هذه المسألة.

٣ - إذا كانت $T=G_1\times G_2\times \ldots \times G_n$ فأثبت أنه لكل i، $i=1,2,\ldots n$ يوجد تشاكل ϕ_i من T على G_i. أوجد نواة ϕ_i.

٤ - لتكن G زمرة، $T=G\times G$.

(أ) أثبت أن $D=\{(g,g)|g\in G\}$ زمرة متماثلة مع G.

(ب) أثبت أن D ناظمية في T إذا وفقط إذا كانت G إبدالية.

٥ - لتكن G زمرة إبدالية منتهية. أثبت أن G متماثلة مع حاصل الضرب المباشر لزمر سيلو الجزئية فيها.

٦ - لتكن B,A زمرتين دوريتين رتبتيهما n,m على الترتيب. أثبت أن $A\times B$ دورية إذا وفقط إذا كان n,m أوليين نسبيا.

٧ - استخدم نتيجة المسألة (٦) لإثبات مبرهنة الباقي الصينية وهي أنه إذا كان n,m عددين صحيحين وأوليين نسبيا وكان v,u أي عددين صحيحين فإننا نستطيع إيجاد عدد صحيح x بحيث يكون $x=u \bmod m$ و $x=v \bmod n$.

٨ - أورد مثالا لزمرة G وزمر جزئية ناظمية $N_1,\ldots N_n$ بحيث تكون $G=N_1N_2\ldots N_n$ و $N_i\cap N_j=(e)$ حيث $i\neq j$ ورغم ذلك فإن G لا تساوي حاصل الضرب المباشر الداخلي للزمر الجزئية الناظمية $N_1,\ldots,N_n$.

٩ ـ أثبت أن G هي عبارة عن حاصل الضرب المباشر الداخلي للزمر الجزئية الناظمية $N_1, N_2, \ldots, N_n$ إذا وفقط إذا كان :

(أ) $G = N_1 N_2 \ldots N_n$

(ب) $N_i \cap (N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n) = (e), i=1,2,\ldots n$

١٠ ـ لتكن G زمرة و $K_1 \ldots K_n$ زمر ناظمية جزئية في G . لنفرض أن $K_1 \cap K_2 \ldots \cap K_n = (e)$. ليكن $V_i = G/K_i$. برهن وجود تماثل من G إلى $V_1 \times V_2 \ldots \times V_n$.

١١* ـ لتكن G زمرة إبدالية منتهية بحيث تحتوي على زمرة جزئية H_0 و $H_0 \neq (e)$ كما أن H_0 محتواة في كل زمرة جزئية H ، $H \neq (e)$. أثبت أن G يجب أن تكون دورية . ماذا تستطيع أن تقول عن o(G) ؟

١٢ ـ لتكن G زمرة إبدالية منتهية. أثبت، باستخدام المسألة ١١ ، أن G متماثلة مع زمرة جزئية من حاصل الضرب المباشر لعدد منته من الزمر الدورية المنتهية.

١٣ ـ أورد مثالاً على زمرة G منتهية وغير إبدالية بحيث تحتوي G على زمرة جزئية H_0 ، $H_0 \neq (e)$ كما أن $H_0 \subset H$ لكل الزمر الجزئية H ، $H \neq (e)$ في G .

١٤ ـ أثبت أن أية زمرة رتبتها p^2 ، p عدد أولي، إما أنها دورية أو أنها متماثلة مع حاصل الضرب المباشر لزمرتين دوريتين رتبة كل منهما p .

١٥* ـ لتكن $G = A \times A$ حيث A زمرة دورية رتبتها p ، p عدد أولي. ما هو عدد التماثلات الذاتية للزمرة G ؟

١٦ ـ صف مركز الزمرة G ، حيث $G = K_1 \times \ldots \times K_n$ بدلالة مركز K_i لكل i .

١٧ ـ إذا كانت $G = K_1 \times \ldots \times K_n$ وكان $g \in G$. فصف.

$N(g) = \{x \in G \mid xg = gx\}$.

١٨ ـ إذا كانت G زمرة منتهية وكانت $N_1, \ldots, N_n$ زمرًا جزئية ناظمية في G بحيث أن $G = N_1 N_2 \ldots N_n$ و $o(G) = o(N_1)\, o(N_2) \ldots o(N_n)$. فأثبت أن G هي عبارة عن حاصل الضرب المباشر للزمر الجزئية الناظمية $N_1, \ldots, N_n$.

(٢ - ١٤) الزمر الإبدالية المنتهية

نختتم هذا الفصل بمناقشة ووصف لبنية الزمر الإبدالية المنتهية. إن النتيجة التي سنتوصل إليها هي مبرهنة تقليدية مشهورة غالبا ما يشار إليها بالمبرهنة الأساسية للزمر الإبدالية المنتهية كما أنها نتيجة وافية تماما وذلك بسبب قطعيتها، كما أن من النادر جدًّا أن نحصل على نتيجة محكمة مثل هذه. وبهذه النتيجة يكشف النقاب عن بنية الـزمـر الإبدالية المنتهية وبواسطتها تكون لدينا وسيلة لدراسة أية مسألة حول الزمر الإبدالية المنتهية كما أن لها بعض النتائج الحسابية، فعلى سبيل المثال، إن أحد نتائجها هو ذلك الإحصاء الدقيق لعدد الزمر الإبدالية غير المتماثلة الموجودة من رتبة معينة.

إن من الواجب أن نضيف هنا أن هذا الوصف للزمر الإبدالية المنتهية ليس بذلك القدر من العمومية ومع ذلك، فإننا نحصل على مبرهنة ذات نتائج ملموسة. وكما سنرى في البنـد (٤ـ٥) فإننا سنصف تماما جميع الزمر الإبدالية المولدة بمجموعة منتهية من العناصر ـ إن هذا الوضع لن يغطي فقط حالة الزمر الإبدالية المنتهية ولكن أكثر من ذلك بكثير.

الآن نذكر نص هذه المبرهنة الأساسية:

مبرهنة (٢ - ١٤ - ١)

كل زمرة إبدالية منتهية هي حاصل ضرب مباشر لزمر دورية.

البرهـان

إن الخطوة الأولى هي تقليص المسألة إلى مسألة أسهل قليلا. لقد نوَّهنا في البند السابق (أنظر مسألة ٥ بند ٢ـ١٣) بأن أية زمرة إبدالية منتهية هي عبارة عن حاصل الضرب المباشر لزمر سيلو الجزئية فيها. فإذا عرفنا أن كل واحدة من زمر سيلو الجزئية هي عبارة عن حاصل ضرب مباشر لزمر دورية فإننا نستطيع ضم هذه النتائج لزمر سيلو الجزئية مع بعضها لنجد أن G عبارة عن حاصل ضرب مباشر لزمر دورية ولهذا فإنه يكفي إثبات المبرهنة للزمر الإبدالية التي رتبها p^n، حيث p عدد أولي.

لذلك نفرض أن G زمرة إبدالية رتبتها p^n . إن غايتنا هي إيجاد عناصر $a_1,a_2,\ldots,a_k \in G$ بحيث يمكن كتابة كل عنصر $x \in G$ بطريقة وحيدة على الصيغة $x=a_1^{\alpha_1}a_2^{\alpha_2}\ldots a_k^{\alpha_k}$. لاحظ أنه إذا كان هذا صحيحا وكانت رتبة كل من $a_1,\ldots,a_k$ هي $p_1^{n_1},\ldots,p^{n_k}$ ، على الترتيب حيث $n_1 \geq n_2 \geq \ldots \geq n_k$ فإن الرتبة العظمى لأي عنصر في G ستكون p^{n_1} (برهن ذلك). إن هذا يعطينا إشارة لكيفية البدء بإيجاد العناصر $a_1,\ldots,a_k$ التي نحن بصدد البحث عنها. إن الطريقة المقترحة وَفْقًا لهذا هي أننا نفرض أن a_1 عنصر من أعلى رتبة في G . كيف نختار a_2؟ حسنًا، إذا كانت $A=(a_1)$ زمرة جزئية مولدة بالعنصر a_1 ، عندئذ فإن a_2 يُصوَّر إلى عنصر من أعلى رتبة في G/A_1 ، فإذا استطعنا بنجاح استغلال هذا لإيجاد a_2 المناسب وإذا كانت $A_2=(a_2)$ فإن a_3 يُصوَّر إلى عنصر من رتبة أعلى في G/A_1A_2 وهكذا، باستخدام هذا كدليل لنا نستطيع تركيز التفكير في البرهان.

ليكن a_1 عنصرًا من G بحيث يكون من أعلى رتبة ممكنة هي p^{n_1} ، ولتكن $A_1=(a_1)$. الآن نختار b_2 في G بحيث تكون رتبة صورة b_2 (التي هي $\bar{b}_2$) أكبر ما يمكن في G/A_1 ولتكن p^{n_2} . لما كانت رتبة $\bar{b}_2$ تقسم رتبة b_2 ، ولما كانت رتبة a_1 عظمى لذا فإنه يجب أن يكون لدينا $n_1 \geqslant n_2$. لكي نحصل على الضرب المباشر للزمرتين A_1 و (b_2) يجب علينا إثبات أن $A_1\cap(b_2)=(e)$ وقد لا يكون هذا صحيحا بسبب الاختيار المبدئي للعنصر b_2 ولهذا قد نكون مجبرين على تكييف العنصر b_2 . لنفرض الآن أن $A_1\cap(b_2)\neq(e)$ ، بما أن $b_2^{p^{n_2}} \in A_1$ وبما أنه هو القوة الأولى للعنصر b_2 التي تجعله يقع في A_1 (وذلك وَفْقًا لطريقة اختيارنا للعنصر b_2) فإنه يكون لدينا $b_2^{p^{n_2}}=a_1^i$ ولذلك فإن

$$(a_1^i)^{p^{n_1-n_2}} = (b_2^{p^{n_2}})^{p^{n_1-n_2}} = b_2^{p^{n_1}} = e$$

وبالتالي فإن $a_1^{ip^{n_1-n_2}} = e$ ولما كانت رتبة a_1 هي p^{n_1} ، لذا فإنه يجب أن يكون لدينا $p^{n_1} | ip^{n_1-n_2}$ ولذلك فإن $p^{n_2}|i$ وهكذا وبتذكر ما هو العدد i يكون لدينا

إذا كان $a_1^{jp^{n2}} = a_1^i = b_2^{p^{n2}}$. إن هذا يفيد بأنه $a_2 = a_1^{-jp^{n2}}$ فإن $a_2^{p^{n2}} = e$. إن العنصر a_2 هو ذلك العنصر الذي نبحث عنه بالفعل . لتكن $A_2=(a_2)$. إننا ندعي أن $A_1 \cap A_2=(e)$ لأنه إذا كان $a_2^t \in A_1$ ولما كان $a_2=a_1^{-j}b_2$ لذا فإننا نجد أن $(a_1^{-j}b_2)^t \in A_1$ وبناءً عليه فإن $b_2^t \in A_1$. إن هذه العلاقة الأخيرة تحتم أن يقسم p^{n2} العدد t وذلك وَفْقًا لاختيار b_2 . ولما كان $a_2^{p^{n2}}=e$ فإنه يجب أن يكون لدينا $a_2^t=e$ أي أن $A_1 \cap A_2=(e)$.

ونتقدم خطوة أخرى في برنامجنا الذي أوجزناه سابقا. ليكن $b_3 \in G$ بحيث يُصوَّر إلى عنصر ذي رتبة عظمى في G/A_1A_2 . فإذا كانت رتبة صورة b_3 في G/A_1A_2 هي p^{n_3} فإننا ندعي أن $n_3 \leq n_2 \leq n_1$. لماذا؟

استنادًا إلى اختيار n_2 نجد أن $b_3^{p^{n2}} \in A_1$. ولذلك بالتأكيد أن $b_3^{p^{n2}} \in A_1A_2$ وهكذا فإن $n_3 \leq n_2$.

ولما كان $b_3^{p^{n3}} \in A_1A_2$ ، لذا فإن $b_3^{p^{n_3}} = a_1^{i_1}a_2^{i_2}$ إننا ندعي أن $p^{n_3}|i_1$ وأن $p^{n_3}|i_2$. لأنه، لما كان $b_3^{p^{n2}} \in A_1$ فإننا نجد

$$(a_1^{i_1}a_2^{i_2})^{p^{n2-n_3}} = (b_3^{p^{n3}})^{p^{n2-n_3}} \equiv b_3^{p^{n2}} \in A_1$$

وهذا يفيد بأن $a_2^{i_2 p^{n_2-n_3}} \in A_1$ ومن ثم فإن $p^{n_2} | i_2 p^{n_2-n_3}$ أي أن $p^{n_3} | i_2$ كما أن $b_3^{p^{n_1}} = e$ ، لذلك فإن $(a_1^{i_1}\ a_2^{i_2})^{p^{n_1-n_3}} = b_3^{p^{n_1}} = e$ وهذا يعني أن $a_1^{i_1 p^{n_1-n_3}} \in A_2 \cap A_1 = (e)$ وبالتالي فإن $a_1^{i_1 p^{n_1-n_3}} = e$ ، أي أن، $p^{n_3} | i_1$.

ليكن $i_1 = j_1 p^{n_3}, i_2 = j_2 p^{n_3}$ عندئذ $b_3^{p^{n_3}} = a_1^{j_1 p^{n_3}}\ a_2^{j_2 p^{n_3}}$. لنفرض أن $a_3 = a_1^{-j_1}\ a_2^{-j_2}\ b_3$ وأن $A_3 = (a_3)$. لاحظ أن $a_3^{p^{n_3}} = e$. إننا ندعي أن $A_3 \cap (A_1\ A_2) = (e)$ لأنه إذا كان $a_3^t \in A_1 A_2$ فإن : $(a_1^{-j_1}\ a_2^{-j_2}\ b_3)^t \in A_1\ A_2$ وهذا يقتضي أن $b_3^t \in A_1\ A_2$ ولكن، عندئذ، $p^{n_3}|t$ وبالتالي فإن لدينا $a_3^t = e$ وذلك لأن $a_3^{p^{n_3}} = e$ وبعبارة أخرى يكون لدينا $A_3 \cap (A_1\ A_2) = (e)$.

وبالاستمرار على هذا النحو نحصل على زمر جزئية دورية $A_1=(a_1), A_2=(a_2), \ldots, A_k=(a_k)$ التي رتبها هي $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$ على الترتيب حيث $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_k$ بحيث تكون $G=A_1A_2\ldots A_k$ كما أنه لكل i يكون $A_i \cap (A_1A_2\ldots A_{i-1}) = (e)$.

إن هذا يجعل لكل عنصر $x \in G$ تمثيلاً وحيدًا على الصيغة $x=a_1'a_2'\ldots a_k'$ حيث $a_1' \in A_1, a_2' \in A_2, \ldots, a_k' \in A_k$ ، وبعبارة أخرى، تكون G هي حاصل الضرب المباشر للزمر الجزئية الدورية $A_1, A_2, \ldots, A_k$. وبهذا ينتهي البرهان.

تعريف

إذا كانت G زمرة إبدالية رتبتها p^n حيث p عدد أولي، وكانت $G=A_1 \times A_2 \times \ldots \times A_k$ حيث كل من A_i زمرة دورية رتبتها p^{n_i} ، $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_k$ عندئذ يطلق على الأعداد الصحيحة $n_1, n_2, \ldots, n_k$ ***لا متغيرات الزمرة G (Invariants)*** .

إن مجرد تسميتنا للأعداد الصحيحة أعلاه لا متغيرات الزمرة G لا يعني على الإطلاق أن هذه هي فقط اللامتغيرات للزمرة G ، بمعنى أنه من الممكن أن ننسب مجموعات مختلفة من اللامتغيرات إلى الزمرة G وسنثبت حالاً أن لا متغيرات G وحيدة حقًا وأنها تصف الزمرة G بصورة تامة.

لاحظ أمرًا آخر حول لا متغيرات G ذلك هو أنه إذا كانت $G=A_1 \times \ldots \times A_k$ حيث A_i زمرة دورية رتبتها p^{n_i} ، $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_k$ فعندئذ $o(G)=o(A_1)o(A_2)\ldots o(A_k)$ لذلك نجد أن

$$p^n = p^{n_1}p^{n_2}\ldots p^{n_k}=p^{n_1+n_2+\ldots+n_k}$$

وبالتالي فإن $n=n_1+n_2+...+n_k$ وبعبارة أخرى، $n_1,n_2,...,n_k$ تزودنا **بتجزيء** للعدد n ولقد تطرقنا إلى هذا المفهوم سابقا عند دراستنا لفصول ترافق زمر التناظر.

قبل دراسة وحدانية لا متغيرات الزمرة G ، يجب علينا أن نوضح أن العناصر $a_1,a_2,...,a_k$ والزمر الجزئية $A_1,A_2,...,A_k$ المولدة بهذه العناصر والتي وردت سابقا لتعطي تفريقا للزمرة G إلى حاصل الضرب المباشر للزمر الدورية ليست وحيدة. دعنا نوضح ذلك بالمثال البسيط الآتي.

لتكن $G=\{e,a,b,ab\}$ هي الزمرة الإبدالية التي رتبتها 4 ، حيث $a^2=b^2=e$ و $ab=ba$ ، عندئذ $G=A\times B$ ، حيث $A=(a)$ و $B=(b)$ هما الزمرتان الدوريتان التي رتبة كل منهما 2 ، بيد أن لدينا تفريقا آخر للزمرة G إلى حاصل الضرب المباشر وهو $G=C\times B$ ، حيث $B=(b), C=(ab)$ وهكذا فإنه حتى في هذه الزمرة التي رتبتها صغيرة جدًّا نستطيع الحصول على تفريقين مختلفين لها كضرب مباشر لزمرتين دوريتين. إن إدعائنا ـ الذي سنثبته الآن ـ هو أنه بينما تكون هذه الزمر الجزئية الدورية غير وحيدة *فإن رتبها، بخلاف ذلك، هي وحيدة.*

تعريـف

إذا كانت G زمرة إبدالية وكان s هو أي عدد صحيح فإننا نعرف $G(s)=\{x\in G\,|\,x^s=e\}$.

وحيث إن G زمرة إبدالية لذا فإن من الواضح أن $G(s)$ زمرة جزئية من G .

تمهيدية (٢-١٤-١)

إذا كانت G', G زمرتين إبداليتين متماثلتين فإن $G'(s), G(s)$ متماثلتان، لأي عدد صحيح s .

البرهـان

ليكـن ϕ تماثـلاً من G على G' . إنـنـا ندعـي أن ϕ يطبق $G(s)$ تماثليا على $G'(s)$. **أولاً** نثـبـت أن $\phi(G(s))\subset G'(s)$ فإذا كان $x\in G(s)$ فإن $x^s=e$ ولـذلـك فإن $\phi(x^s)=\phi(e)=e'$ ولكن $\phi(x^s)=\phi(x)^s$ ، لذا فإن $\phi(x)^s=e'$ وبـالـتـالي فإن $\phi(x)\in G'(s)$ أي أن $\phi(G(s))\subset G'(s)$.

ومن ناحية أخـرى، إذا كان $u'\in G'(s)$ فإن $(u')^s=e'$ ، ولكن، بما أن ϕ تطبيق غامـر فإن $u'=\phi(y)$ حيث $y\in G$ وبالتالي فإننا نجد $e'=(u')^s=\phi(y)^s=\phi(y^s)$ ولما كان ϕ أحاديا لذلك يكون لدينا $y^s=e$ وبالتالي فإن $y\in G(s)$. وهكذا فإن ϕ يطبق $G(s)$ على $G'(s)$. وحيث إن ϕ أحادي وغامر وهو تشاكل من $G(s)$ و $G'(s)$ لذلك فإن $G(s)$ و $G'(s)$ متماثلتان.

الآن ننتقل إلى التمهيدية الآتية:

تمهيدية (٢-١٤-٢)

لتـكـن G زمـرة إبـدالـية رتـبـتـهـا p^n حيث p عدد أولي ولـنـفـرض أن $G=A_1\times A_2\times\ldots\times A_k$ حيث كل من $A_i=(a_i)$ زمـرة دورية، $i=1,2,..k$ رتـبـتـهـا P^{n_i} ، $n_1\geq n_2\geq\ldots\geq n_k>0$ فإذا كان m عددًا صحيحـا بحيث أن $n_t>m\geq n_{t+1}$ فعندئذ:

$$G(p^m)=B_1\times\ldots\times B_t\times A_{t+1}\times\ldots\times A_k$$

حيث B_i زمـرة دورية مولـدة بالـعـنـصر $a_i^{p^{n_i-m}}$ ورتـبـتهـا هي p^m لكـل $i\leq t$ كما أن رتبة $G(p^m)$ هي p^u حيث

$$u=mt+\sum_{i=t+1}^{k} n_i$$

البرهـان

أولا، وقبل كل شيء، إننا ندعي أن $A_{t+1},\ldots,A_k$ جميعها محتواة في $G(p^m)$ لأنه لما كان $m\geq n_{t+1}\geq\ldots\geq n_k>0$ وإذا كان $j\geq t+1$ فإن

$a_j^{p^m}=(a_j^{p^{n_j}})^{p^{m-n_j}}=e$ ولـــذلـــك فإن A_j حيث $j\geqslant t+1$ محتواة في $G(p^m)$.

ثانيا، إذا كان $i\leqslant t$ فإن $n_i>m$ كما أن $(a_i^{p^{n_i-m}})^{p^m}=a_i^{p^{n_i}}=e$ ولـــذلـــك فإن كل عنصر من الصيغة $a_i^{p^{n_i-m}}$ ينتمي إلى $G(p^m)$ ومن ثم فإن الزمرة B_i التي يولدها هذا العنصر هي أيضـــا محتـــواة في $G(p^m)$ ولمـــا كانت $B_1,\ldots,B_t,A_{t+1},\ldots,A_k$ جميعهـــا محتـــواة في $G(p^m)$ لذلك فإن حاصل ضربها (الذي هو مباشر، لأن حاصل الضرب $A_1A_2\ldots A_k$ مباشر أيضًا) يكون في $G(p^m)$ وبالتالي فإن $G(p^m)\supset B_1\times\ldots\times B_t\times A_{t+1}\times\ldots\times A_k$.

ومـن ناحـية أخـــرى إذا كان $x=a_1^{\lambda_1}a_2^{\lambda_2}\ldots a_k^{\lambda_k}$ عنصرًا في $G(p^m)$ ونـــظرًا لأنـــه يحقق العـلاقـة $x^{p^m}=e$ لذا فإننـا نضع $e=x^{p^m}=a_1^{\lambda_1 p^m}\ldots a_k^{\lambda_k p^m}$ ولـكـن حاصـــل ضرب الزمر الجزئية $A_1,\ldots,A_k$ مباشر ولهذا فإننا نحصل على $a_1^{\lambda_1 p^m}=e,\ldots,a_k^{\lambda_k p^m}=e$.

وهكـــذا فإن رتبـــة a_i والتي هي p^{n_i} يجب أن تقسم $\lambda_i p^m$ ، حيث $i=1,2,\ldots,k$ فإذا كانت $i\geqslant t+1$ فإن هذا يكـــون صحيحـــا من تلقـــاء ذاتـــه مهـــما كان اختيار $\lambda_{t+1},\ldots,\lambda_k$ لأن $m\geqslant n_{t+1}\geqslant\ldots\geqslant n_k$ ولهـــذا فإن $p^{n_i}|p^m$ ، $i\geqslant t+1$. ومـع ذلـك، فإننا نحـــصـــل من أجـــل $i\leqslant t$ ومـــن كون $p^{n_i}\,|\,\lambda_i p^m$ على $p^{n_i-m}|\lambda_i$ وبـالتـالـي نجـد أن $\lambda_i=\upsilon_i p^{n_i-m}$ حيث υ_i عدد صحيح ما. وبـالتعويض عن λ_i لكـــل i في الـــتـــعـــبـــير $x=a_1^{\lambda_1}\ldots a_k^{\lambda_k}$ نجد أن

$$x=a_1^{\upsilon_1 p^{n_1-m}}\ldots a_t^{\upsilon_t p^{n_t-m}}a_{t+1}^{\lambda_{t+1}}\ldots a_k^{\lambda_k}$$

إن هذا يعني أن $x\in B_1\times\ldots\times B_t\times A_{t+1}\times\ldots\times A_k$

الآن، لما كانت رتـبـــة B_i هي p^m لكـــل i ولمـــا كانـــت $o(A_i)=p^{n_i}$ وأيضـــا لما كانت $G(p^m)=B_1\times\ldots\times B_t\times A_{t+1}\times\ldots A_k$. لذا فإن

$$o(G(p^m))=o(B_1)o(B_2)\ldots o(B_t)o(A_{t+1})\ldots.o(A_k)$$
$$=\underbrace{p^m p^m\ldots p^m}_{\text{t من المرات}}p^{n_{t+1}}\ldots p^{n_k}$$

فإذا كانت $o(G(p^m))=p^u$ فإن

$$u=mt+\sum_{i=t+1}^{k}n_i$$

وبهذا يتم برهان التمهيدية.

نتيجة

إذا كانت G كما وردت في التمهيدية السابقة فإن $o(G(p))=p^k$.

البرهان

بتطبيق التمهيدية السابقة وذلك عندما $m=1$ وعندئذ $t=k$ ومن ثم فإن $u=1.k=k$ وبناء عليه نجد أن $o(G(p))=p^k$.

إن لدينا الآن المعلومات اللازمة لإثبات وحدانية اللامتغيرات للزمرة الإبدالية التي رتبتها p^n .

مبرهنة (٢ ـ ١٤ ـ ٢)

تكون الزمرتان الإبداليتان من الرتبة p^n متماثلتين إذا وفقط إذا كان لهما نفس اللامتغيرات. وبعبارة أخرى، إذا كانت رتبة كل من الزمرتين الإبداليتين هي p^n وكانت $G=A_1\times\ldots\times A_k$ ، حيث كل من A_i زمرة دورية رتبتها p^{n_i} كما أن $n_1\geqslant n_2\geqslant\ldots\geqslant n_k>0$ وإذا كانت $G'=B'_1\times\ldots\times B'_s$ ، حيث كل من B'_i زمرة دورية رتبتها p^{h_i} كما أن $h_1\geqslant h_2\geqslant\ldots\geqslant h_s>0$ ، فإن G و G' متماثلتان إذا وفقط إذا كان $k=s$ و $n_i=h_i$ لكل i .

البرهان

إن برهان أحد اتجاهي المبرهنة بسيط جدًّا ذلك هو أنه إذا كان للزمرتين G و G' نفس اللامتغيرات فإنهما متماثلتان لأنه عندئذ $G=A_1\times\ldots\times A_k$ ، حيث $A_i=(a_i)$ زمرة دورية رتبتها p^{n_i} كما أن $G'=B'_1\times\ldots\times B'_k$ حيث $B'_i=(b'_i)$ زمرة دورية رتبتها p^{n_i} ثم أرسل G على G' بواسطة التطبيق

$$\phi(a_1^{\alpha_1}\ldots a_k^{\alpha_k}) = (b_1')^{\alpha_1}\ldots(b_k')^{\alpha_k}$$

سنترك للقارىء التحقق من أن ϕ هو، بالفعل، تماثل من G على G' .

ولبرهان الاتجاه المعاكس، لنفرض $G=A_1\times\ldots\times A_k$ وأن $G'=B_1'\times\ldots\times B_s'$ ، حيث A_i و B_i' كما وردتا أعلاه، كما أنهما زمرتان دوريتان مولدتان بالعنصرين a_i و b_i' ورتبتاها p^{n_i} و p^{h_i} ، $n_1\geqslant n_2\geqslant\ldots\geqslant n_k>0$ و $h_1\geqslant h_2\geqslant\ldots\geqslant h_s>0$ ونريد إثبات أنه إذا كانت G و G' متماثلتين فإن $k=s$ و $n_i=h_i$ لكل i .

لنفرض الآن أن G و G' متماثلتان، عندئذ، استنادًا إلى تمهيدية (٢ ـ ١٤ ـ ١) فإن $G(p^m)$ و $G'(p^m)$ يجب أن تكونا متماثلتين لأي عدد صحيح $m\geqslant 0$. ولذلك يجب أن تتساوى رتبتاهما. لنرى الآن ماذا يحدث، في الحالة الخاصة، عندما $m=1$. أي ما هي المعلومات التي يمكن الحصول عليها عندما $o(G(p))=o(G'(p))$. استنادًا إلى نتيجة التمهيدية (٢ ـ ١٤ ـ ٢) نجد أن $o(G(p))=p^k$ و $o(G(p))=p^s$ ولذلك فإن $p^k=p^s$ ومن ثم فإن $k=s$. وبالتالي فإننا نعرف، على الأقل، أن عدد اللامتغيرات للزمرتين G و G' هو نفسه.

لنفرض الآن أن $n_i\neq h_i$ وذلك لعدد ما i وليكن t هو أول الأعداد i التي يكون من أجلها $n_t\neq h_t$. هنا يمكن أن نفرض أن $n_t>h_t$. ليكن $m=h_t$ ولنعتبر الزمرتين الجزئيتين $H=\{x^{p^m}|x\in G\}$ و $H'=\{(x')^{p^m}|x'\in G\}$ من G و G' على الترتيب.

إن H', H متماثلتان وذلك لأن G', G كذلك. ندرس الآن لامتغيرات H', H . لما كانت $G=A_1\times\ldots\times A_k$ ، حيث $A_i=(a_i)$ زمرة دورية رتبتها p^{n_i} فإننا نجد أن

$$H=C_1\times\ldots\times C_t\times\ldots\times C_r$$

حيث $C_i=(a_i^{p^m})$ زمرة دورية رتبتها p^{n_i-m} كما أن r يخضع للشرط $n_r>m=h_t\geqslant n_{r-1}$ وهكذا فإن لا متغيرات H هي $n_1-m,n_2-m,\ldots,n_r-m$ كما أن عددها هو r ، $r\geqslant t$.

أيضـا لما كانـت $G'=B'_1\times\ldots\times B'_s$ ، حيث $B'_i=(b'_i)$ زمـرة دورية رتبـتـهـا p^{h_i} ، لذا فإننا نجد أن $H'=D'_1\times\ldots\times D'_{t-1}$ حيث $D'_i=((b'_i)^{p^m})$ زمـرة دورية رتبتهـا p^{n_i-m} .

وبالتالي فإن لا متغيرات H' هي $h_1-m,h_2-m,\ldots,h_{t-1}-m$ كما أن عددها هو $t-1$.

ولكن H و H' متماثلتان، وكما رأينا أعلاه، فإنه لابد أن يكون لهما العدد نفسه من اللامتغيرات، وهكذا فإن افتراضنا بأن $n_i>h_i$ لعدد ما i قادنا إلى اختلاف في عدد اللامتغيرات لهاتين الزمرتين وعليه فإن $n_i=h_i$ لكل i ، وبهذا يتم برهان المبرهنة.

يتضح لنـا وذلك كنتيجة مباشرة من المبرهنة الأخيرة أنه يمكن تفريق الزمرة الإبدالية التي رتبتها p^m وذلك بطريقة وحيدة ـ كحاصل ضرب مباشر لزمر جزئية دورية **(إن المقصود هنا هو وحدانية رتب الزمر الجزئية الدورية فقط)** ولذلك فإن اللامتغيرات هي، بالفعل، لا متغيرات الزمرة G كما أنها تعيّن G تماما.

إذا كانـت $n_1\geqslant n_2\geqslant\ldots\geqslant n_k>0$ وكـان $n=n_1+n_2+\ldots+n_k$ هو أي تجزيء للعدد n فإننا، عندئذ، نستطيع وبسهولة تكوين الزمرة الإبدالية التي رتبتها p^n والتي تكون لا متغيراتها هي $n_1\geqslant n_2\geqslant\ldots\geqslant n_k>0$ ولإنجاز هذا، لتكن A_i هي الزمرة الدورية التي رتبتها p^{n_i} ولتكن $G=A_1\times\ldots\times A_k$ كحاصل الضرب المباشر الخارجي للزمر $A_1,\ldots,A_k$. عندئذ فإن لا متغيرات الزمرة G هي $n_1\geqslant n_2\geqslant\ldots\geqslant n_k>0$ وذلك استنادًا إلى تعـريفها. وأخيرًا إذا كان هناك تجزيئان مختلفان للعدد n فإنه ينشأ عن ذلك زمرتان إبداليتان غير متماثلتين رتبة كل منهما p^n . إن هذا يتضح من مبرهنة (٢ـ١٤ـ٢) ومن ثم يكون لدينا المبرهنة الآتية.

مبرهنة (٢ـ١٤ـ٣)

إن عدد الزمر الإبدالية غير المتماثلة والتي رتبة كل منها p^n ، حيث p عدد أولي، يساوي عدد تجزيئات العدد n .

إن نتيجة المبرهنة (٢-١٤-٣) لا تعتمد على العدد الأولي p ، بل إنها تعتمد فقط على العدد n ولذلك، وعلى سبيل المثال، فإن عدد الزمر الإبدالية غير المتماثلة والتي رتبة كل منها 2^4 هو نفسه ذلك العدد لتلك الزمر التي رتبة كل منها 3^4 أو 5^4 . . الخ .

ولما كان يوجد 5 تجزيئات للعدد 4 هي :

$$4=4,\ 3+1,\ 2+2,\ 2+1+1,\ 1+1+1+1$$

لذلك فإنه يوجد 5 زمرا إبدالية غير متماثلة رتبة كل منها p^4 ، لأي عدد أولي p .

وحيث إن أية زمرة إبدالية منتهية هي عبارة عن حاصل الضرب المباشر لزمر سيلو الجزئية فيها وحيث إن أي زمرتين إبداليتين تكونان متماثلتين إذا وفقط إذا كانت زمر سيلو الجزئية فيهما متماثلات لهذا تكون لدينا النتيجة الآتية .

نتيجـة

إن عدد الـزمـر الإبدالية غير المتماثلة التي رتبة كل منها هي $p_1^{\alpha_1}...p_r^{\alpha_r}$ ، حيث p_i أعـداد أولية مختلفـة ، $\alpha_i>0$ هو $p(\alpha_1)p(\alpha_2)...p(\alpha_r)$ حيث $p(u)$ هو عدد تجزيئات العدد u .

مسائــل

١ - إذا كانت G زمرة إبدالية رتبتها p^n ، p عدد أولي وكانت $n_1\geqslant n_2\geqslant...\geqslant n_k>0$ هي لا متغيرات الزمرة G فأثبت أن الرتبة العظمى لأي عنصر في G هي p^{n_1} .

٢ - إذا كانـت G زمــرة وكــانــت $A_1,...,A_k$ زمــرًا جزئية ناظمية من G بحيث إن $A_i\cap(A_1A_2...A_{i-1})=(e)$ لكـــل i . فأثبت أن G هي حاصـل الضرب المبـاشر لـ $A_1,...,A_k$ إذا كانت $G=A_1A_2...A_k$.

٣ - باستخدام مبرهنة (٢-١٤-١)، أثبت أنه إذا كانت G زمرة إبدالية منتهية تحتوي على زمرتين جزئيتين رتبتاهما m و n فإنها تحتوي على زمرة جزئية رتبتها، على الأقل، هي المضاعف المشترك للعددين m و n .

٤ - صف جميع الزمر الإبدالية المنتهية التي رتبتها

(أ) 2^6 (ب) 11^6 (جـ) 7^5 (د) $2^4.3^4$

٥ - وضح كيف تحصل على جميع الزمر الإبدالية التي رتبة كل منها $2^3.3^4.5$

٦ - إذا كانت G زمرة إبدالية رتبتها p^n وكانت لا متغيراتها هي $n_1 \geqslant n_2 \geqslant ... \geqslant n_k > 0$ وكانت H زمرة جزئية من G و $H \neq (e)$. فأثبت أنه إذا كانت $h_1 \geq h_2 \geq ... \geq h_s > o$ هي لا متغيرات H فإن $k \geq s$ ، كما أنه لكل i يكون $h_i \leq n_i$ حيث $i = 1, ..., s$.

إذا كانت G زمرة إبدالية وكانت $\bar{G}$ هي مجموعة كل التشاكلات من الزمرة G إلى مجموعة الأعداد المركبة غير الصفرية بالنسبة لعملية الضرب وإذا كان $\phi_1, \phi_2 \in \bar{G}$ فإننا نعرف $\phi_1 . \phi_2$ كما يلي $(\phi_1 . \phi_2)(g) = \phi_1(g)\phi_2(g)$ لكل $g \in G$.

٧ - أثبت أن $\bar{G}$ زمرة إبدالية بالنسبة للعملية المعرفة .

٨ - إذا كان $\phi \in \bar{G}$ وكانت G منتهية . فأثبت أن $\phi(g)$ هو جذر وحدة لكل $g \in G$.

٩ - إذا كانت G زمرة دورية منتهية . فأثبت أن $\bar{G}$ دورية وأن $o(G) = o(\bar{G})$ ومن ثم فإن $G, \bar{G}$ متماثلتان .

١٠ - إذا كان $g_1 \neq g_2$ ، g_2 ، حيث g_1 عنصران من زمرة إبدالية منتهية G . فأثبت أنه يوجد $\phi \in \bar{G}$ بحيث يكون $\phi(g_1) \neq \phi(g_2)$.

١١ - إذا كانت G زمرة إبدالية منتهية . فأثبت أن $o(G) = o(\bar{G})$ وأن G متماثلة مع $\bar{G}$.

١٢ - إذا كان $\phi \in \bar{G}$ و $\phi \neq 1$ حيث G زمرة إبدالية . فأثبت أن $\sum_{g \in G} \phi(g) = o$.

مسائل إضافية

لا يوجد علاقة بين ترتيب هذه المسائل وبين ترتيب البنود في هذا الفصل وذلك فيما يتعلق بحلول المسائل . كما أنه لم يرد أي تلميح إلى صعوبة أية مسألة .

١ - (أ) إذا كانت G زمرة إبدالية منتهية عناصرها $a_1, ..., a_n$. فأثبت أن $a_1 a_2 ... a_n$ عنصر مربعه هو العنصر المحايد .

(ب) في الفقرة (ا) إذا كانت G لا تحتوي على أي عنصر رتبته تساوي 2 أو أكثر من عنصر واحد رتبته تساوي 2 . فأثبت أن $a_1 a_2 ... a_n = e$.

(جـ) إذا كانت G تحتوي على عنصر واحد، y ، رتبته تساوي 2 . فأثبت أن $a_1 a_2 ... a_n = y$.

(د) (مبرهنة ويلسون Wilson) إذا كان p عددًا أوليا. فأثبت أن $(p-1)! \equiv -1 \pmod{p}$.

٢ ـ إذا كان p عدداً أوليا فرديا وإذا كان

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} = \frac{a}{b}$$

حيث b, a عددان صحيحان. فأثبت أن $p|a$ وإذا كان $p>3$ فأثبت أن $p^2|a$.

٣ ـ إذا كان p عددًا أوليا فرديا و $a \not\equiv 0 \pmod{p}$ فإنه يقال عن العدد a إنه **راسب تربيعي** (Quadratic residue) للعدد p إذا كان يوجد عدد صحيح x بحيث يكون $x^2 \equiv a \pmod{p}$. برهن ما يلي:

(ا) إن الرواسب التربيعية للعدد p تكون زمرة جزئية Q من زمرة الأعداد الصحيحة غير الصفرية قياس p وذلك بالنسبة لعملية الضرب.

(ب) $o(Q) = (\frac{p-1}{2})$

(جـ) إذا كان $q \in Q$ وكان $n \notin Q$ (n **يدعى غير راسب** non residue) فإن nq غير راسب.

(د) إذا كان كل من n_1, n_2 غير راسب فإن $n_1 n_2$ راسب تربيعي.

(هـ) إذا كان a راسبا تربيعيا للعدد p ، فإن $a^{\frac{p-1}{2}} \equiv +1 \pmod{p}$

٤ ـ أثبت أنه يوجد في مجموعة الأعداد الصحيحة قياس p ، حيث p عدد أولي، حلول عددها على الأكثر هو n للمعادلة $x^n \equiv 1 \pmod{p}$ وذلك لكل عدد صحيح n .

٥ ـ أثبت أن مجموعة الأعداد الصحيحة غير الصفرية قياس p هي زمرة دورية بالنسبة لعملية الضرب وذلك عندما يكون p عددًا أوليا.

٦ ـ أورد مثالا لزمرة غير إبدالية يكون فيها $(xy)^3 = x^3y^3$ وذلك لجميع العناصر x,y .

٧ ـ إذا كانت G زمرة إبدالية منتهية. فأثبت أن عدد حلول المعادلة $x^n = e$ في G ، حيث $n|o(G)$ ، هو مضاعف للعدد n .

٨ ـ أثبت ما ورد في المسألة (٧) ولكن بدون أن نفرض أن G إبدالية.

٩ ـ أوجد التماثلات الذاتية لزمرتي التناظر S_4, S_3 من الدرجتين 3 و4 على الترتيب.

تعريـــف

*يقـــال إن الـــزمـــرة G **قابلة للحـــل** (Solvable) إذا كان يوجـــد زمـــر جزئية $G=N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_r=(e)$ بحيث تكون N_i ناظمية في N_{i-1} و N_{i-1}/N_i إبدالية .*

١٠ - برهن على أن الزمرة الجزئية من زمرة قابلة للحل وكذلك الصورة التشاكلية لزمرة قابلة للحل يجب أن تكونا قابلتين للحل .

١١ - إذا كانـت G زمـرة و N زمـرة جزئـية ناظمية في G . بحيث إن كلا من N و G/N قابلة للحل . فأثبت أن G قابلة للحل .

١٢ - إذا كانت G زمرة وكانت A زمرة جزئية من G و N زمرة جزئية ناظمية في G . فأثبت أنه إذا كانت كل من A و N قابلة للحل فإن AN قابلة للحل كذلك .

١٣ - لنفرض أن G زمرة ولنعرف المتتابعة $G^{(i)}$ من الزمر الجزئية في G كما يلي :

(أ) $G^{(1)}$ هي زمـرة المبـدلات الجزئية في G ، أي الزمرة الجزئية في G المولدة بجميع العناصر $aba^{-1}b^{-1}$ حيث $a,b \in G$.

(ب) $G^{(i)}$ هي زمرة المبدلات الجزئية في $G^{(i-1)}$ عندما $i>1$. برهن ما يلي :

(١) $G^{(i)}$ زمرة جزئية ناظمية في G لكل i .

(٢) G قابلة للحل إذا وفقط إذا كانت $(G)^{(k)}=(e)$ وذلك لعدد ما k ، $k \geq 1$.

١٤ - برهن على أن الـزمـرة القـابلة للحـل تحـتوي دائـما على زمـرة جزئية ناظمية إبدالية M و $M \neq (e)$.

لنفرض أن G زمرة ولنعرف المتتابعة $G_{(i)}$ من الزمر الجزئية في G كما يلي :

(أ) $G_{(1)}$ هي زمرة المبدلات الجزئية في G .

(ب) $G_{(i)}$ هي الـزمـرة الجـزئية من G المـولـدة بجميع العنـاصر $aba^{-1}b^{-1}$ حيث $a \in G$, $b \in G_{(i-1)}$.

يقال إن الزمرة G **معدومة القوى** (Nilpotent) إذا كان $G_{(k)}=(e)$ وذلك لعدد ما k ، $k \geq 1$.

١٥ - (أ) أثبت أن $G_{(i)}$ زمرة جزئية ناظمية في G لكل i كما أن $G_{(i)} \supset G^{(i)}$.

(ب) إذا كانت G معدومة القوى . فأثبت أنها يجب أن تكون قابلة للحل .

(جـ) أورد مثالا لزمرة قابلة للحل لكنها ليست معدومة القوى .

١٦ ـ أثبت أن أية زمرة جزئية من زمرة معدومة القوى هي معدومة القوى كذلك. وأن أية صورة تشاكلية لزمرة معدومة القوى هي معدومة القوى كذلك.

١٧ ـ أثبت أن أية صورة تشاكلية لا تساوي (e) لزمرة معدومة القوى تحتوي على مركز غير تافه.

١٨ ـ (ا) أثبت أن أية زمرة رتبتها p^n، p عدد أولي، يجب أن تكون معدومة القوى.

(ب) إذا كانت G معدومة القوى وكانت H زمرة جزئية من G بحيث أن $H \neq G$. فأثبت أن $N(H) \neq H$ حيث إن $N(H)=\{x \in G \mid xHx^{-1}=H\}$.

١٩ ـ إذا كانت G زمرة منتهية. فأثبت أن G تكون معدومة القوى إذا وفقط إذا كانت G هي حاصل الضرب المباشر لزمر سيلو الجزئية فيها.

٢٠ ـ لنفرض أن G زمرة منتهية وH زمرة جزئية من G. ولنعرف على G العلاقة الآتية «*إذا كانت* B,A *زمرتين جزئيتين فإن* A *ترافق* B *نسبة إلى* H *إذا كانت* $B=x^{-1}Ax$، $x \in H$».

برهن على ما يلي:

(ا) إن هذه العلاقة هي علاقة تكافؤ على مجموعة الزمر الجزئية في G

(ب) إن عدد الزمر الجزئية في G المرافقة للزمرة الجزئية A نسبة إلى H يساوي دليل $N(A) \cap H$ في H.

٢١ ـ (ا) إذا كانت G زمرة منتهية وكانت P هي زمرة سيلو الجزئية من نوع p. فأثبت أن P هي زمرة سيلو الجزئية الوحيدة من نوع p في $N(P)$.

(ب) إذا كانت P هي زمرة سيلو الجزئية من نوع p في G وكان $a^{p^k}=e$، فعندئذ إذا كان $a \in N(P)$ فأثبت أن a يجب أن يكون في P.

(جـ) أثبت أن $N(N(P))=N(P)$.

٢٢ ـ (ا) إذا كانت G زمرة منتهية وP هي زمرة سيلو الجزئية من نوع p في G. فأثبت أن عدد الزمر الجزئية المرافقة للزمرة الجزئية P في G ليس مضاعفا للعدد p.

(ب) بتجزيء فصل ترافق الزمرة الجزئية P وذلك باستعمال الترافق نسبة إلى P. برهن على أن فصل ترافق P يحتوي على زمر جزئية مختلفة عددها

$1+kp$. (**إرشاد**: استخدم فقرة (ب) من مسألة (٢٠) ومسألة (٢١). لاحظ أن هذا مع مسألة (٢٤) يزودنا ببرهان بديل لمبرهنة (٢-١٢-٣) والجزء الثالث من مبرهنة سيلو).

٢٣ - (أ) إذا كانت P هي زمرة سيلو الجزئية من نوع p في G وكانت B زمرة جزئية من G رتبتها p^k وكانت B ليست محتواة في إحدى مرافقات P . فأثبت أن عدد مرافقات P في G هو مضاعف للعدد p .

(ب) باستخدام فقرة (أ) ومسألة (٢٢). أثبت أن B يجب أن تكون محتواة في إحدى مرافقات P .

(جـ) برهن على أن أي زمرتين جزئيتين من زمر سيلو من نوع p في G يجب أن تكونا مترافقتين في G (إن هذا برهان آخر لمبرهنة (٢-١٢-٢) والجزء الثاني من مبرهنة سيلو).

٢٤ - ضم المسألتين (٢٢)، (٢٣) لتحصل على برهان آخر لجميع أجزاء مبرهنة سيلو.

٢٥ - باستخدام النتائج التي حصلنا عليها في هذا الفصل. أثبت أن أية زمرة رتبتها أقل من 60 هي إما زمرة رتبتها عدد أولي أو أنها تحتوي على زمرة جزئية ناظمية غير تافهة وذلك بمناقشتك لكل حالة على انفراد.

٢٦ - باستخدام نتيجة المسألة (٢٥). أثبت أن أية زمرة رتبتها أقل من 60 قابلة للحل.

٢٧ - أثبت أن المعادلة $x^2ax=a^{-1}$ قابلة للحل بالنسبة إلى x في الزمرة G إذا وفقط إذا كان a مكعبا لعنصر ما في G .

٢٨ - برهن على أن (123) ليس مكعبا لأي عنصر في S_n .

٢٩ - أثبت أن $xax=b$ قابلة للحل بالنسبة إلى x في G إذا وفقط إذا كان ab مربعا لعنصر ما في G .

٣٠ - إذا كانت G زمرة وكانت رتبة العنصر $a\in G$ منتهية وكان عدد العناصر المرافقة للعنصر a في G منته أيضا. فأثبت مرافقات العنصر a تولد زمرة جزئية ناظمية منتهية في G .

٣١ - أثبت أن أية زمرة لا يمكن كتابتها على هيئة اتحاد عناصر زمرتين جزئيتين فعليتين فيها .

٣٢ - أثبت أن أية زمرة G هي اتحاد ثلاث زمر جزئية فعلية فيها إذا وفقط إذا كانت للزمرة G صورة تشاكلية هي زمرة غير دورية رتبتها 4 .

٣٣ - ليكن p عدداً أوليا و Z_p هي مجموعة الأعداد الصحيحة قياس p بالنسبة لعمليتي الجمع والضرب قياس p . ولتكن G هي الزمرة $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ حيث $a,b,c,d \in Z_p$ ، $ad-bc=1$ ولتكن $C=\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}$ ولتكن $LF(2,p)=G/C$.

(ا) أوجد رتبة $LF(2,p)$

(ب) برهن على أن $LF(2,p)$ زمرة بسيطة وذلك إذا كان $p \geqslant 5$.

٣٤ - أثبت أن $LF,(2,5) \approx A_5$ ، حيث A_5 هي زمرة التناوب من الدرجة 5 .

٣٥ - لتكن $G=LF(2,7)$. استنادًا إلى مسألة (٣٣) فإن G زمرة بسيطة رتبتها 168 . عين تماما كم عدد زمر سيلو الجزئية من نوع 2 ، نوع 3 ، نوع 7 في G .

قراءة إضافية

- **Burnside, W.** *Theory of Groups of finite order,* 2nd Ed. Cambridge, England: Cambridge University Press, 1911; New York: Dover Publications, 1955
- **Hall, Marshall.** *Theory of groups.* New york: The Macmillan Company, 1961.

مواضيع للمناقشة في الصف

- **Alperin J.L.** "A Classification of N-abelian Groups", *Canadian Journal of Mathematics,* XXI (1969), 1238-1244.
- **Mckay, James H.** "Another prof. of Couchy's group theorem." *American Mathematical Monthly,* 66 (1956), 119.
- **Segal, L.E.** "The automorphisms of symmetric groups". *Bulletin of The American Mathematical Society,* 46 (1940), 565.

٣

نظرية الحلقات

• تعاريف وأمثلة على الحلقات • بعض الأصناف الخاصة من الحلقات • التشاكلات • المثاليات والحلقات الخارجة • مزيد من المثاليات والحلقات الخارجة • حقل خوارج القسمة للحلقة التامة • الحلقات الإقليدية • حلقة إقليدية خاصة • حلقات كثيرات الحدود • كثيرات الحدود على حقل الأعداد النسبية • حلقات كثيرات الحدود على الحلقات الإبدالية

(٣-١) تعاريف وأمثلة على الحلقات

كما بينا في الفصل الثاني، هناك بعض النظم الجبرية التي تعتبر حجر الأساس لموضوع يدعى اليوم بالجبر الحديث. في هذه المرحلة من تطور دراستنا نكون قد تعلمنا بعض الشيء عن واحد من هذه النظم ألا وهي الزمر.

وفي هذا الفصل سندرس نظامًا آخر هو الحلقات. كما عرفنا سابقًا فإن الفكرة المجردة للزمرة يرجع أصلها إلى مجموعة تطبيقات أو تبديلات عناصر مجموعة. وبالمقارنة فإن الحلقات تنبثق من مصدر آخر أكثر أُلْفَةً لنا هو مجموعة الأعداد الصحيحة.

كما سنرى فإن الحلقات مصممة لتكون حالة عامة للأوجه الجبرية للأعداد الصحيحة المعتادة. سيتضح لنا في الفقرة القادمة أن الحلقة تختلف تمامًا عن الزمرة في أنها نظام ذو عمليتين هما عمليتا الجمع والضرب. وبالرغم من ذلك فإن دراستنا

للحلقات ستتبع نفس النمط الذي اتبعناه في الزمر فستحتاج لما يقابل التشاكل، الزمر الجزئية الناظمية والزمر الخارجة الخ . .

ومـع الخـبرة التي اكتسبناها أثناء دراستنا للزمر سنتمكن من تقديم التعاريف الضرورية مع مبرهنات منتهين ببرهنة نتائج مشوقة ومهمة حول مواضيع رياضية أَلِفْنَاها من قبل. وكي نضرب مثلا على ذلك سنبرهن لاحقًا في هذا الكتاب وباستعمال المادة المعطاة هنا بأنه من المستحيل تقسيم زاوية مقدارها ٦٠° إلى ثلاثة أقسام متساوية باستعمال المسطرة والفرجار فقط.

تعريف

تسمى المجموعة غير الخالية R حلقة تجميعية (associative ring) إذا كان بالإمكان تعريف عمليتين على R نرمز لهما بـ + و . على الترتيب بحيث أنه لجميع العناصر a,b,c في R :

١ ـ $a+b$ يكون في R

٢ ـ $b+a=a+b$

٣ ـ $a+(b+c)=(a+b)+c$

٤ ـ يوجد عنصر 0 في R بحيث أن $a=a+0$ (لكل عنصر a في R)

٥ ـ يوجد عنصر $-a$ في R بحيث $0=(-a)+a$

٦ ـ $a.b$ يكون في R

٧ ـ $(a.b).c=a.(b.c)$

٨ ـ $a.b+a.c=a.(b+c)$ و $(b+c).a=b.a+c.a$ (قانونا التوزيع).

- المسلمات من ١ إلى ٥ تنص على أن R زمرة إبدالية بالنسبة إلى العملية + والتي ندعوها الجمع.
- المسلمات ٦ إلى ٧ تبين أن R مجموعة مغلقة بالنسبة إلى العملية التجميعية. والتي نسميها الضرب.
- أما المسلمة ٨ فتعمل على ربط تلك العمليتين المعرفتين على R .

عندما نتحدث عن الحلقات فإننا نعني الحلقات التجميعية، أما الحلقات غير التجميعية أي الحلقات التي لا تحقق المسلمة رقم ٧ فإنها تُدرس في الرياضيات ولكننا لن نتمكن من التطرق إليها.

من الممكن أن يوجد أو لايوجد عنصر في R نرمز له بـ1 بحيث $a=1.a=a.1$ لجميع العناصر a في R وفي حالة وجود مثل هذا العنصر تطلق على R **حلقة بعنصر الوحدة** (ring with unit element).

إذا كانت عملية الضرب في R تحقق $b.a=a.b$ لجميع a,b في R تسمى R **حلقة إبدالية** (commutative ring).

قبل أن نستمر في التعرف على بعض خواص الحلقات، نتوقف لاستعراض بعض الأمثلة والتي من خلالها سوف نعرف أنواعًا مختلفةً ومهمة من الحلقات.

مثال (٣-١-١)

لتكن R هي مجموعة الأعداد الصحيحة (integers) الموجبة والسالبة والصفر، + هي عملية الجمع الاعتيادية و. هي عملية الضرب المألوفة للأعداد الصحيحة. عندئذ R هي حلقة إبدالية بعنصر وحدة.

مثال (٣-١-٢)

لتكن R هي مجموعة الأعداد الصحيحة الزوجية (even integers) بالنسبة لعمليتي الجمع والضرب الاعتياديتين. عندئذ R هي حلقة إبدالية ولكن بدون عنصر وحدة.

مثال (٣-١-٣)

لتكن R هي مجموعة الأعداد النسبية (المنطّقة) (rational numbers) بالنسبة لعمليتي الجمع والضرب الاعتياديتين. عندئذ R هي حلقة إبدالية بعنصر

وحدة. ولكن بالإضافة إلى ذلك لاحظ أن عناصر R المختلفة عن الصفر تكون زمرة إبدالية بالنسبة لعملية الضرب. الحلقة التي تحقق هذه الخاصة الآنفة الذكر تسمى **حقلاً** (field).

مثال (٣-١-٤)

لتكن R مجموعة الأعداد الصحيحة قياس 7 (integers mod 7) بالنسبة لعمليتي الجمع والضرب قياس 7 بمعنى أن عناصر R هي الرموز السبعة $\bar{6},\bar{5},\bar{4},\bar{3},\bar{2},\bar{1},\bar{0}$ حيث إن:

١ - $\bar{k}=\bar{j}+\bar{i}$ حيث k هو باقي قسمة j+i عند تقسيمه على 7 (مثالا على ذلك، $\bar{2}=\bar{5}+\bar{4}$ لأن 4+5=9 والذي عند تقسيمه على 7 يكون باقي القسمة 2).

٢ - $\bar{m}=\bar{j}.\bar{i}$ حيث m هو باقي قسمة ji عند تقسيمه على 7 (وبالتالي فإن $\bar{1}=\bar{3}.\bar{5}$ لأن 3.5=15 وباقي قسمته على 7 هو 1).

على الطالب أن يتحقق من أن R هي حلقة إبدالية بعنصر وحدة. بل يمكننا نثبت أكثر من ذلك ونعني، بما أن

$$\bar{1}.\bar{1}=\bar{1}=\bar{6}.\bar{6}$$
$$\bar{2}.\bar{4}=\bar{1}=\bar{4}.\bar{2}$$
$$\bar{3}.\bar{5}=\bar{1}=\bar{5}.\bar{3}$$

لذلك فإن عناصر R غير المساوية للصفر تكون زمرة إبدالية بالنسبة لعملية الضرب وبالتالي فإن R هي حقل، وبما أنه يحوي على عدد مُنتهٍ من العناصر لذلك يسمى **حقلاً منتهياً** (finite field)

مثال (٣-١-٥)

لتكن R هي مجموعة الأعداد الصحيحة قياس 6 بالنسبة لعمليتي الجمع والضرب قياس 6 . إذا رمزنا لعناصر R بالرموز $\bar{0},\bar{1},...,\bar{5}$ يمكننا أن نلاحظ أن

$\bar{0}=\bar{3}.\bar{2}$ مع أن $\bar{2}\neq\bar{0}$ و $\bar{3}\neq\bar{0}$. *لذلك فإنه من الممكن في حلقة* R *أن يكون* $a.b=0$ *دون أن يكون* $a=0$ *أو* $b=0$. إن هذا لا يمكن أن يحدث في الحقل (أنظر مسألة ١ في نهاية بند ٣-٢)، ولذلك فمن المؤكد أن R في هذا المثال ليست حقلاً.

جميع الأمثلة التي وردت حتى الآن كانت لحلقات إبدالية. الآن نورد مثالا على حلقة غير إبدالية.

مثال (٣ - ١ - ٦)

لتكن R مجموعة جميع الرموز

$$\alpha_{11}e_{11}+\alpha_{12}e_{12}+\alpha_{21}e_{21}+\alpha_{22}e_{22}=\sum_{i,j=1}^{2}\alpha_{ij}e_{ij}$$

حيث إن جميع α_{ij} هي أعداد نسبية (منطّقة) كما أن

(١) $$\sum_{i,j=1}^{2}\alpha_{ij}e_{ij}=\sum_{i,j=1}^{2}\beta_{ij}e_{ij}$$

إذا وإذا فقط لجميع $\alpha_{ij}=\beta_{ij},\ i,j=1,2$

(٢) $$\sum_{i,j=1}^{2}\alpha_{ij}e_{ij}+\sum_{i,j=1}^{2}\beta_{ij}e_{ij}=\sum_{i,j=1}^{2}(\alpha_{ij}+\beta_{ij})e_{ij}$$

(٣) $$\left(\sum_{i,j=1}^{2}\alpha_{ij}e_{ij}\right)\left(\sum_{i,j=1}^{2}\beta_{ij}e_{ij}\right)=\sum_{i,j=1}^{2}\gamma_{ij}e_{ij}$$

حيث

$$\gamma_{ij}=\sum_{v=1}^{2}\alpha_{iv}\beta_{vj}=\alpha_{i1}\beta_{1j}+\alpha_{i2}\beta_{2j}$$

عملية الضرب هذه تبدو لأول وهلة معقدة. ولكنها مبنية على قواعد بسيطة نسبيًا وبالتحديد، إنك تضرب $\sum\alpha_{ij}e_{ij}$ بـ $\sum\beta_{ij}e_{ij}$ شكليًا وذلك بضرب الحدود بعضها ببعض

ثم تجمع الحدود المتشابهة على أن تأخذ في نظر الاعتبار العلاقات $e_{ij}.e_{kl}=0$ عندما $j\neq k$ و $e_{ij}.e_{jl}=e_{il}$ (طبعًا أولئك القراء الذين سبق وأن درسوا بعض مواضيع الجبر الخطي سيعرفون هذا المثال على أنه حلقة جميع المصفوفات من النوع 2×2 على حقل الأعداد النسبية).

لتوضيح عملية الضرب، لتكن $a=e_{11}-e_{21}+e_{22}$ و $b=e_{22}+3e_{12}$ عندئذ

$$\begin{aligned}a.b&=(e_{11}-e_{21}+e_{22}).(e_{22}+3e_{12})\\&=e_{11}.e_{22}+3e_{11}.e_{12}-e_{21}.e_{22}-3e_{21}.e_{12}\\&+e_{22}.e_{22}+3e_{22}.e_{12}\\&=0+3e_{12}-0-3e_{22}+e_{22}+0\\&=3e_{12}-3e_{22}+e_{22}=3e_{12}-2e_{22}.\end{aligned}$$

لاحظ أن $e_{11}.e_{12}=e_{12}$ بينما $e_{12}.e_{11}=0$. لذلك فإن عملية الضرب في R ليست إبدالية. كذلك من الممكن أن تكون $u.v=0$ مع أن $v\neq 0$ و $u\neq 0$.

على الطالب أن يتحقق من أن R هي حلقة حقًا. وهي تدعى حلقة المصفوفات النسبية من نوع 2×2 . وسوف تحتل هذه الحلقة حيزا غير قليل مما سوف يأتي من هذا الكتاب.

مثال (٣-١-٧)

لتكن C مجموعة كل الرموز (α, β) حيث α, β أعداد حقيقية. نعرف المساواة

$$(\alpha,\beta) = (\gamma,\delta) \tag{1}$$

إذا وإذا فقط إذا كان $\alpha=\gamma$ و $\beta=\delta$

في C نعرف عملية الجمع بالطريقة التالية: لتكن $X=(\alpha,\beta)$ و $Y=(\gamma,\delta)$ عندئذ

$$X+Y=(\alpha,\beta)+(\gamma,\delta)=(\alpha+\gamma,\beta+\delta) \tag{2}$$

لاحظ أن $X+Y$ موجود في C . تؤكد هنا أن C هي زمرة إبدالية بالنسبة لهذه العملية عنصرها المحايد هو $(0,0)$ و $(-\alpha,-\beta)$ هو المعكوس الجمعي للعنصر (α,β) .

والآن وبعد أن زودنا C بعملية جمع فإننا نحتاج إلى عملية ضرب لنجعل منها حلقة. وتحقق ذلك بالتعريف التالي: ليكن $X=(\alpha,\beta)$ و $Y=(\gamma,\delta)$ عنصرين في C عندئذ:

$$X.Y=(\alpha,\beta).(\gamma,\delta)=(\alpha\gamma-\beta\delta,\alpha\delta+\beta\gamma) \quad (3)$$

لاحظ أن

$$X.Y = Y.X$$

كذلك

$$X.(1,0) = (1,0)\,.\,X = X$$

لذا فإن (1,0) هو عنصر الوحدة في C .

ومرة أخرى نلاحظ أن $X.Y\in C$. كذلك إذا كان $X=(\alpha,\beta)\neq(0,0)$ فإنه نظرًا لكون α,β عددين حقيقيين غير مساويين للصفر، فإن $\alpha^2+\beta^2\neq 0$ وهكذا فإن

$$Y=\left(\frac{\alpha}{\alpha^2+\beta^2},\frac{-\beta}{\alpha^2+\beta^2}\right)$$

هو عنصر في C .

أخيرا نرى أن:

$$(\alpha,\beta)\,.\left(\frac{\alpha}{\alpha^2+\beta^2},\frac{-\beta}{\alpha^2+\beta^2}\right)=(1,0)$$

وهكذا نكون قد أثبتنا أن C حقل. إذا كتبنا (α,β) على الصيغة $\alpha+\beta i$ فإنه يمكن للقارىء أن يتحقق من أن C هي مجرد صيغة مخفية للأعداد المركبة (Complex numbers) التي نألفها.

مثال (٣-١-٨)

هذا المثال الأخير غالبا ما يطلق عليه إسم حلقة **الرباعيات الحقيقية** (real quaternions) . أول من وصف هذه الحلقة هو الرياضي الإيرلندي هاملتون (Hamilton) . في البداية استعملت هذه الحلقة بصورة موسعة في دراسة الميكانيكا،

أما اليوم فإن فائدتها الرئيسة تكمن في كونها مثالاً مهماً بالرغم من أنها مازالت تلعب دورًا فعالاً في الهندسة ونظرية الأعداد.

لتكن Q هي مجموعة جميع الرموز $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ حيث إن جميع الأعداد $\alpha_3,\alpha_2,\alpha_1,\alpha_0$ أعداد حقيقية. نقول إن الرمزين $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ و $\beta_0+\beta_1 i+\beta_2 j+\beta_3 j$ متساويان إذا وفقط إذا كان $\alpha_t=\beta_t$ لجميع قيم t وهي 3,2,1,0 . لكي نجعل من Q حلقة يجب أن نعرف عملية جمع + وعملية ضرب . لجميع عناصرها. ومن أجل ذلك نعرف

أولاً:

لكل عنصرين Y, X في Q حيث

$$X = \alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k \text{ و } Y = \beta_0+\beta_1 i+\beta_2 j+\beta_3 k$$

يكون

$$X + Y = (\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k) + (\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)$$
$$= (\alpha_0+\beta_0)+(\alpha_1+\beta_1)i+ (\alpha_2+\beta_2)j+(\alpha_3+\beta_3)k$$

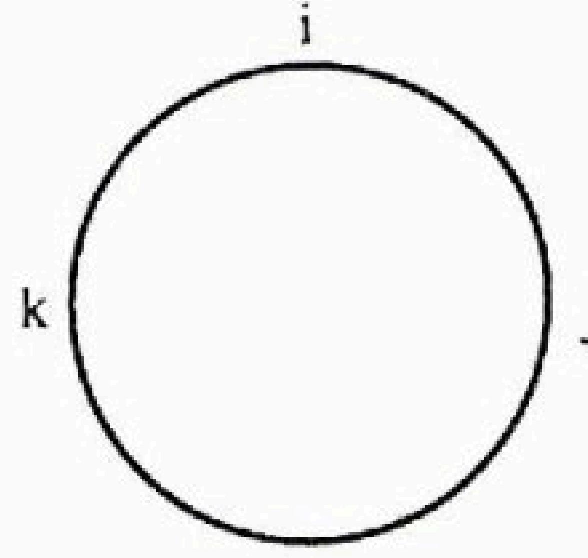
وثانيًا:

$$X . Y = (\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k) . (\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)$$
$$= (\alpha_0\beta_0 -\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3) + (\alpha_0\beta_1 +\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)i$$
$$+ (\alpha_0\beta_2 +\alpha_2\beta_0+\alpha_3\beta_1-\alpha_1\beta_3)j + (\alpha_0\beta_3 +\alpha_3\beta_0+\alpha_1\beta_2-\alpha_2\beta_1)k.$$

والحق يقال إن صيغة الضرب هذه تبدو صعبة ولكنها في الحقيقة ليست بهذا التعقيد إنها تأتي من ضرب مثل هذين الرمزين شكليًا وتجميع الحدود باستعمال العلاقات

$$i^2=j^2=k^2=ijk= -1, ij= -ji=k, jk= -kj=i, ki= -ik=j$$

الجزء الأخير من هذه العلاقات يسمى جدول الضرب للوحدات الرباعية، ويمكننا تذكره باستعمال الشكل



فعندما تدور باتجاه عقارب الساعة يمكنك استنباط حاصل الضرب، مثلاً:

$$ij=k,\ jk=i,\ ki=j$$

بينما إذا درت عكس عقارب الساعة تحصل على سالب حواصل الضرب أعلاه.
لاحظ أن العناصر $\pm 1, \pm i, \pm j, \pm k$ تكون زمرة غير إبدالية رتبتها 8 نسبة لعملية الضرب هذه. في الحقيقة هذه هي الزمرة التي أطلقنا عليها زمرة الوحدات الرباعية (group of quaternion units) في الفصل الثاني.

يمكن للقارىء أن يثبت أن Q هي حلقة غير إبدالية والتي فيها
$0=0+0i+0j+0k$ و $1=1+0i+0j+0k$
يعملان عمل الصفر وعنصر الوحدة على التوالي. والآن إذا كان

$$X=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k\neq 0$$

فإن الأعداد $\alpha_0,\alpha_1,\alpha_2,\alpha_3$ ليست كلها أصفارًا، ولأن هذه الأعداد حقيقية فإن

$$\beta = \alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2+\neq 0$$

وهكذا فإن

$$Y=\frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i-\frac{\alpha_2}{\beta} j-\frac{\alpha_3}{\beta} k\in Q$$

وبإجراء حسابات بسيطة يمكننا أن نبين أن $X.Y=1$. لذلك فإن عناصر Q غير الصفرية تكون زمرة غير إبدالية بالنسبة لعملية الضرب. الحلقة التي تكوّن عناصرها غير الصفرية زمرة تسمى **حلقة قسمة** (division ring) أو **حقلاً تخالفياً** (Skew-field) بالطبع إن حلقة القسمة الإبدالية هي حقل. في هذا المثال أوردنا

Q كحلقة قسمة ولكنها ليست حقلاً. يوجد الكثير من الأمثلة على حلقات القسمة غير الإبدالية. ولكننا كي نقدم مثالا آخر على ذلك سنبتعد كثيرًا عن مسار عرض المادة وأخيرا نقول إن دراسة طبيعة حلقات القسمة ومحاولات تصنيفها تكون جزءاً مهما من علم الجبر.

(٣-٢) بعض الأصناف الخاصة من الحلقات

تبين الأمثلة التي نُوقشت في البند (٣-١) وبوضوح أنه بالرغم من أن الحلقات هي تعميم مباشر للأعداد الصحيحة إلا أن بعض الحقائق الحسابية التي أَلِفْنَاها في الأعداد الصحيحة قد لا تتحقق في الحلقات عامة. مثلا رأينا أنه يمكن أن يكون حاصل الضرب a.b صفرًا دون أن يكون أي من a أو b مساويا للصفر. كذلك هناك أمثلة كثيرة a.b≠b.a . كل هذه الحالات لا تتفق مع خبرتنا السابقة.

ولسهولة الكتابة فإننا من الآن فصاعدًا سوف نلغي النقطة في a.b ونكتفي بكتابة حاصل الضرب على الصيغة ab

تعريف

*إذا كانت R حلقة إبدالية و a عنصرًا في R لا يساوي صفراً، فإنه يقال إن a **قاسم للصفر** (Zero-divisor) إذا وُجد عنصر b لا يساوي صفرًا في R بحيث أن $ab=0$*

تعريف

*تسمى الحلقة الإبدالية **حلقة تامة** (integral domain) إذا كانت لا تحوي قواسمًا للصفر.*

إن الأعداد الصحيحة هي مثال على الحلقة التامة.

تعريف

***حلقة القسمة** (division ring) هي الحلقة التي تكون عناصرها غير الصفرية زمرة بالنسبة لعملية الضرب.*

سوف نرمــز لعنصر الــوحـدة بالنسبـة لعملية الضرب بالـرمـز 1 ولمعكـوس العنصر a تحت عملية الضرب بالرمز a^{-1}

والآن نعرف شيئًا ذا أهمية عظمى ، ألا وهو الحقل.

تعريف

الحقل (field) هو حلقة قسمة إبدالية .

في أمثلتنا في البند (٣-١) عرضنا مثالا على حلقة قسمة غير إبدالية وهي حلقة الربـاعيات الحقيقية والحقـول التـالية: الأعـداد النسبية، الأعداد المركبة والأعداد الصحيحة قياس 7 . الفصل الخامس من هذا الكتاب سيخصص لدراسة الحقول وخصائصها.

نود أن نكون قادرين على إجراء الحسابات في الحلقات بطريقة مشابهة لما نجريه في الأعـداد الحقيقية واضعـين في أذهـاننـا دائـما أن هنـاك فروقات - قد يحصل أن $ab \neq ba$ أو أننـا لا نستـطيع إجـراء عملية القسمـة. ومن أجل ما ذكرناه نبرهن على التمهيدية التالية التي تؤكد بأن بعض الأمور التي ترغب أن تكون صحيحة في الحلقات هي حقًا كذلك.

تمهيدية (٣-٢-١)

إذا كانت R حلقة ، فإنه لجميع a,b في R يكون

(1) $a0 = 0a = 0$

(2) $a(-b) = (-a)b = -(ab)$

(3) $(-a)(-b) = ab$

وإذا كانت R ، بالإضافة إلى ذلك ، تحتوي على عنصر الوحدة 1 فإن

(4) $(-1)a = -a$

(5) $(-1)(-1) = 1$

البرهان

أولا: إذا كان a في R فإن

$$a0 = a(0+0) = a0+a0$$

(باستخدام قانون التوزيع الأيمن) وحيث إن R هي زمرة بالنسبة لعملية الجمع فإن هذه المعادلة تقتضي أن يكون $a0=0$.
وبطريقة مشابهة

$$0a = (0+0)a = 0a+0a$$

وذلك باستخدام قانون التوزيع الأيسر وبذلك نحصل على أن $0a=0$

ثانيًا: من أجل أن نبين أن

$$a(-b) = -(ab)$$

يجب أن نبرهن على أن

$$ab+a(-b) = 0$$

ولكن

$$ab+a(-b) = a(b+(-b)) = a0=0$$

باستعمال قانون التوزيع ونتيجة القسم الأول من هذه التمهيدية. وبالطريقة ذاتها نحصل على أن

$$(-a)b = -(ab)$$

ثالثًا: المساواة

$$(-a)(-b) = ab$$

هي في الحقيقة حالة خاصة من الجزء الثاني، وهنا نركز عليها لأن نظيرها في الأعداد الحقيقية قد سبق التأكيد عليه في تعلّمنا في المراحل المبكرة. لذا فلنبرهنها

$$(-a)(-b) = -(a(-b)) \qquad \text{(من الجزء الثاني)}$$

$$= -(-(ab)) \qquad \text{(من الجزء الثاني)}$$

$$= ab$$

لأن $x = -(-x)$ وهي حقيقة نستنتجها من أنه في أية زمرة

$$(a^{-1})^{-1} = a$$

رابعًا: لنفرض أن R تمتلك عنصر الوحدة 1 عندئذ

$$a+(-1)a=1a+(-1)a=(1+(-1))a=0a=0$$

لذا نحصل على

$$(-1)a = -a$$

وفي الحالة الخاصة إذا كانت $a = -1$ فإن

$$(-1)(-1) = -(-1) = 1$$

وبذلك نكون قد برهنا على الجزء الخامس من التمهيدية.

بعد أن برهنا على هذه التمهيدية ستصبح لنا الحرية من الآن فصاعدًا في التعامل مع السوالب والصفر في حساباتنا كما اعتدنا عليها سابقًا. إن نتيجة التمهيدية (٣-٢-١) تسمح لنا بذلك. للسهولة سنكتب $a+(-b)$ على الصيغة $a-b$.

التمهيدية التي انتهينا من برهنتها لا شك في أنها مفيدة ومهمة إلا أنها ليست مثيرة. لذا دعنا نستمر لنقدم نتائج أكثر أهمية. وقبل أن نفعل ذلك نذكر مبدأ، على الرغم من كونه تافها كليا ولكنه يعطينا سلاحا قويا إذا استُخْدِم بمهارة. هذا المبدأ لا يتعدى التالي: إذا وزع ساعي البريد **١٥٦** رسالة على **١٥٥** صندوق بريد فإن أحد صناديق البريد يجب أن يستلم رسالتين على الأقل. إن هذا لا يبدو أنه أداة فعالة، أليس كذلك؟ ولكنه سيفاجئنا ! بأن الأفكار الرياضية، غالبًا، ما تكون غامضة وصعبة جدا ولكن هذا لا ينطبق على هذا المبدأ البسيط الآنف الذكر. والآن نعطيه الصفة الرسمية ونخصص له إسما هو:

مبـــدأ توزيـع الأمـاكن *The Pigeonhole Principle*

إذا وزعنـا *n من الأشياء على m من الأمـاكن وكانت $n>m$ فإن أحد الأماكن سيستلم شيئين على الأقل.*

هنـاك صياغـة مكـافئة غالبًا ما سنستعملها، وهي : إذا وزعنا n من الأشياء على n من الأماكن بحيث إن أيًا من الأماكن لا يستلم أكثر من شيء واحد فإن كل مكان يستلم شيئًا واحدًا بالضبط.

الآن نستعمل هذه الفكرة في برهنة التمهيدية التالية.

تمهيدية (٣-٢-٢)
أية حلقة تامة منتهية هي حقل

البرهان

كما نتذكر أن الحلقة التامة هي حلقة إبدالية بحيث $ab=0$ إذا وفقط إذا كان أحد العنصرين على الأقل a أو b يساوي صفرًا. ومن ناحية أخرى الحقل هو حلقة إبدالية بعنصر الوحدة والتي يوجد فيها لكل عنصر غير صفري معكوس ضربي في الحلقة.

لتكن D حلقة تامة منتهية لكي نبرهن على أن D هي حقل يجب علينا
أولاً : أن نجد عنصرًا 1 في D بحيث $a1=a$ لجميع العناصر a في D
ثانيًا: لكل عنصر $a\neq0$ في D نجد عنصراً b في D بحيث $ab=1$.
لتكن $x_1,x_2,\ldots x_n$ هي جميع عناصر D وافرض أن $a\neq o$ في D . لنعتبر العناصر $x_1a,x_2a,\ldots,x_na$ إنها جميعاً في D . ندعي أن هذه العناصر جميعها مختلفة. فلو فرضنا أن $x_ia=x_ja$ في حالة $i\neq j$ ينتج عن ذلك أن $(x_i-x_j)a=0$. ولأن D حلقة تامة و $a\neq0$ لذا نحصل على أن $x_i-x_j=0$ ومن ثم $x_i=x_j$ وهذا يناقض كون $i\neq j$. لذلك فإن $ax_1,ax_2,\ldots,ax_n$ هي n من العناصر المختلفة في D . باستخدام مبدأ توزيع الأماكن فإن هذه العناصر هي جميع عناصر D أو بعبارة أخرى، كل عنصر y في D يمكن أن تكتب على شكل x_ia حيث x_i هو أحد عناصر D .

وبصورة خاصة، لأن $a \in D$ فإن $a = x_{i_0} a$ حيث x_{i_0} هو عنصر في D . لأن D حلقة إبدالية، نحصل على

$$a = x_{i_0} a = a x_{i_0}$$

الآن نسعى لنبرهن على أن x_{i_0} تعمل عمل عنصر الوحدة لجميع عناصر D . ليكن y عنصرًا في D فكما رأينا من قبل $y = x_i a$ لعنصر ما x_i في D . ولذلك

$$y x_{i_0} = (x_i a) x_{i_0} = x_i (a x_{i_0}) = x_i a = y$$

ومن ذلك نستنتج أن x_{i_0} هو عنصر الوحدة في D ونكتبه على شكل 1 . الآن بما أن $1 \in D$ فإنه باستخدام المناقشة السابقة يمكننا أن نكتبه أيضا كمضاعف للعنصر a ، أي أنه يوجد عنصر b في D بحيث أن $1 = ba$. وبهذا نكون قد أتممنا برهنة التمهيدية.

نتيجة

إذا كان p عددًا أوليًا فإن Z_p حلقة الأعداد الصحيحة قياس p تكون حقلاً.

البرهان

باستخدام التمهيدية يكفينا أن نبرهن على أن Z_p هي حلقة تامة ذلك لأنها تحوي على عدد منتهٍ من العناصر. إذا كان a,b عنصرين في Z_p و $ab \equiv 0$ فإن على p أن يقسم العدد الصحيح ab ولكون p عددًا أوليا فإن p يجب أن يقسم إما a أو b . ولكن عندئذ إما أن $a \equiv 0$ قياس p أو $b \equiv 0$ قياس p وبناء عليه فإن أحد العنصرين يساوي صفرًا في Z_p .

النتيجة أعلاه تضمن لنا إيجاد عدد غير منتهٍ من الحقول الحاوية على عدد منتهٍ من العناصر مثل هذه الحقول يُطلق عليها إسم **الحقول المنتهية**. إن الحقول Z_p لا تعطينا جميع الأمثلة على الحقول المنتهية، بل هناك حقول أخرى. وفي الحقيقة إننا سنقدم وصفًا كاملاً لجميع الحقول المنتهية في البند (٧-١).

الآن نورد فرقا مدهشًا بين الحقول المنتهية وحقول مثل الأعداد النسبية، الأعداد الحقيقية، أو الأعداد المركبة والتي نحن أكثر إلمامًا بها.

ليكن F حقلاً منتهيا يحوي على q من العناصر (اعتبر، على سبيل المثال، Z_p الحاوي على p من العناصر). عندما ننظر للحقل F على أنه مجرد زمرة بالنسبة لعملية الجمع، وحيث إن F تحوي على q من العناصر نحصل على

$$\underbrace{a+a+\ldots+a}_{\text{q من المرات}} = qa=0$$

وذلك بالاستعانة بالنتيجة (٢) من المبرهنة (٢-٤-١) حيث a أي عنصر في F. لذلك فإنه في F يكون لدينا qa=0 لعدد صحيح موجب q حتى لو كان $a\neq0$ هذا بالتأكيد لا يمكن أن يحدث في حقل الأعداد النسبية مثلاً. سنبرز هذا الفرق في التعاريف التالية، وبدلاً من أن نحصر الحديث حول الحقول، فإننا سنوسع المجال قليلا ونتحدث عن الحلقات التامة.

تعريف

*يقال للحلقة التامة D إنها **صفرية المميز** (of characteristic 0) إذا كانت العلاقة $ma=0$ حيث $a\neq0$ في D و m عدد صحيح لا تتحقق إلا إذا كان $m=0$.*

وهكذا فإن حلقة الأعداد الصحيحة هي صفرية المميز، كذلك الحلقات المألوفة الأخرى مثل الأعداد الصحيحة الزوجية والأعداد النسبية.

تعريف

*يقال للحلقة التامة D إنها **منتهية المميز** (of finite characteristic) إذا وُجد عدد صحيح موجب m بحيث أن $ma=0$ لجميع العناصر a في D*

إذا كانت D منتهية المميز فإننا نعرف مميز الحلقة التامة D على أنه أصغر عدد صحيح موجب p بحيث $pa=0$ لجميع العناصر a في D . يمكن البرهنة بدون صعوبة تذكر أنه إذا كانت D منتهية المميز، فإن مميزها يجب أن يكون عددًا أوليا (أنظر المسألة ٦ في نهاية هذا البند).

كما أشرنا من قبل أي حقل منتهٍ هو منته المميز، بيد أنه يمكن إيجاد حلقة تامة غير منتهية ولكنها منتهية المميز (أنظر المسألة ٧).

قد يتساءل القارىء: لماذا عرفنا المميز للحلقات التامة فقط وليس لأية حلقة اختيارية؟ إنه لسؤال جد معقول. ربما أن المثال الذي نعطيه الآن يبين ما يحدث في حالة التخلي عن فرضية الحلقة التامة.

لتكن R هي مجموعة جميع الثلاثيات (a,b,c) حيث a في Z_2 الأعداد الصحيحة قياس 2 ، وb في Z_3 ، الأعداد الصحيحة قياس 3 و c هو أي عدد صحيح.

كي نجعل من R حلقة نعرف عملية الجمع + وعملية الضرب . حسب القواعد التالية:

$$(a_1,b_1,c_1)+(a_2,b_2,c_2)=(a_1+a_2,b_1+b_2,c_1+c_2)$$

و

$$(a_1,b_1,c_1)\,.\,(a_2,b_2,c_2)=(a_1a_2,b_1b_2,c_1c_2)$$

إنه لمن السهل التحقق من أن R هي حلقة إبدالية. إنها ليست حلقة تامة لأن:

$$(1,2,0).(0,0,7)=(0,0,0)$$

حيث (0,0,0) هو العنصر الصفري في R . لاحظ أنه في R

$$2(1,0,0)=(1,0,0)+(1,0,0)=(2,0,0)=(0,0,0)$$

بسبب أن عملية الجمع في المركبة الأولى تحصل في Z_2 ، وبالمثل

$$3(0,1,0)=(0,0,0)$$

وأخيرًا فإن العلاقة

$$m(0,0,1)=(0,0,0)$$

لا يمكن أن تتحقق لأي من القيم الصحيحة الموجبة للعدد m .

لذا، استنادًا لما قدمناه أعلاه فيما يخص تعريف المميز نلاحظ أن الحلقة R المعرفة أعلاه ليست صفرية ولا منتهية المميز. والتعريف ليس له أي معنى بالنسبة لهذه الحلقة.

في الحقيقة يمكننا تعميم فكرة المميز لأية حلقة عن طريق تعريفها محليًا نسبة إلى عناصر معينة دون أن نجعلها شاملة للحلقة كلها.

نقول إن لـ R **فتل من درجة** n (n–torsion) حيث n عدد صحيح موجب إذا وجد عنصر $a\neq0$ في R بحيث $na=0$ و $ma\neq0$ لكل $0<m<n$. إذا كانت D حلقة تامة وكان لها فتل من درجة n ولو لعدد واحد موجب فإن D يجب أن تكون منتهية المميز (أنظر مسألة ٨).

مسائل

R هي حلقة في جميع هذه المسائل

١ - إذا كانت d,c,b,a عناصر في R فاحسب $(a+b)(c+d)$

٢ - برهن على أنه إذا كان b,a في R فإن $(a+b)^2=a^2+ab+ba+b^2$ حيث x^2 تعني xx .

٣ - أوجد صيغة مبرهنة ذي الحدين في الحلقة العامة أي عبر عن $(a+b)^n$ حيث n عدد صحيح موجب.

٤ - إذا كان لكل عنصر x في R تتحقق العلاقة $x^2=x$ فبرهن على أن R يجب أن تكون إبدالية (يطلق على مثل هذه الحلقة R حلقة بولينية Boolean ring).

٥ - إذًا كانت R حلقة فباعتبارها مجرد زمرة إبدالية بالنسبة لعملية الجمع لقد عرفنا في الفصل الثاني معنى na حيث a في R و n عدد صحيح . برهن على أنه إذا كانت b,a في R و m,n عددين صحيحين فإنه

$$(na)(ma)=(nm)(ab)$$

٦ - إذا كانت D حلقة تامة منتهية المميز. برهن على أن مميز D يجب أن يكون عددًا أوليًا.

٧ - أورد مثالاً لحلقة تامة تحوي عددًا غير منتهٍ من العناصر، ولكنها منتهية المميز.

٨ - إذا كانت D حلقة تامة وكانت $na=0$ لعنصر $a\neq0$ في D ولعدد صحيح $n\neq0$. برهن على أن D منتهية المميز.

٩ - إذا كانت R نظامًا يحقق جميع شروط الحلقة بعنصر الوحدة مع إمكانية عدم تحقق الشرط $a+b=b+a$. فبرهن على أن المسلمة $a+b=b+a$ يجب أن تتحقق في R وبذلك تكون R حلقة (إرشاد: فك المقدار $(a+b)$ $(1+1)$ بطريقتين).

١٠ - بين أن الحلقة الإبدالية D هي حلقة تامة إذا وفقط إذا كانت المساواة $ab=ac$ تعطينا $b=c$ لجميع العناصر a,b,c في D بحيث $a\neq0$.

١١ - برهن على أن التمهيدية (٣-٢-٢) غير صحيحة إذا أسقطنا فرضية كون الحلقة التامة منتهية.

١٢ - برهن على أن أي حقل هو حلقة تامة.

١٣ - باستعمال مبدأ توزيع الأماكن برهن على أنه إذا كان العددان الصحيحان m,n أوليين نسبيًا وكان b,a أي عددين صحيحين فإنه يوجد عدد صحيح x بحيث $x\equiv a$ قياس m و $x\equiv b$ قياس n (إرشاد: اعتبر بواقي الأعداد $a+(n-1)m,\ldots,a+2m,a+m,a$ عند تقسيمها على n).

١٤ - باستعمال مبدأ توزيع الأماكن. برهن على أن التمثيل العشري لأي عدد نسبي يجب، بعد نقطة ما، أن يكون متكررًا.

(٣-٣) التشاكلات

عند دراستنا للزمر وجدنا أن مفهوم التشاكل كان مثمرًا وهذا يجعلنا نعتقد أن نظيره المناسب في الحلقات قد يقودنا أيضا إلى أفكار مهمة ولكي تستذكر الفكرة، بالنسبة للزمر كنا قد عرفنا التشاكل بأنه تطبيق ϕ بحيث إن :

$$\phi(ab)=\phi(a)\phi(b)$$

ولأن للحلقة عمليتين فإن الامتداد الطبيعي لمثل هذه الصيغة هو في التعريف التالي.

تعريف

يسمى التطبيق ϕ من الحلقة R إلى الحلقة R' ***تشاكلًا*** *(homomorphism) إذا كان*

١ - $\phi(a+b)=\phi(a)+\phi(b)$

٢ - $\phi(ab)=\phi(a)\phi(b)$

لجميع العناصر a,b في R .

كما هي الحالة في الزمر دعنا نؤكد مرة أخرى أن عمليتي الجمع + والضرب · الواقعتين على يسار العلاقات في ١ و٢ هما عمليتان على R بينما تكون العمليتان + و. الواقعتان على اليمين معرفتان على ′R .

من المفيد أن نشير إلى الملاحظة التالية حول التشاكل من الحلقة R إلى حلقة أخرى ′R ، وهي أنه إذا أغفلنا كليا عمليتي الضرب في كلتا الحلقتين، نحصل على تشاكل من R إلى ′R باعتبارهما زمرتين إبداليتين بالنسبة لعملية الجمع المعرفة على كل منهما.

ولذلك فإنه فيما يتعلق بعملية الجمع فإن جميع خصائص التشاكل للزمر والتي سبق وأن بُرهِنت في الفصل الثاني تبقى صحيحة هنا. وعلى سبيل الخصوص نعيد كتابة التمهيدية (٢-٧-٢) في حالة الزمرة الجمعية للحلقة ونحصل على

تمهيدية (٣-٣-١)

إذا كانت ϕ تشاكلًا من R إلى R' فإنه

١ - $\phi(0)=0$

٢ - $\phi(-a)=-\phi(a)$ *لجميع العناصر* a *في* R

تحذير:

إذا كان 1 و $1'$ عنصري الوحدة لعمليتي الضرب في الحلقتين R و R' على الترتيب فليس من الضروري أن يكون $\phi(1)=1'$. ولكن إذا كانت R' حلقة تامة أو R' أية حلقة و ϕ تطبيقا غامرًا onto mapping فإن $\phi(1)=1'$.

في حالة الزمر إذا كان لدينا تشاكل فإننا نربط مع هذا التشاكل مجموعة جزئية معيّنة من الزمرة سميناها نواة التشاكل. تُرى ما هو التعريف المناسب لنواة التشاكل في الحلقات؟ فالحلقة لها عمليتان هما الجمع والضرب ومن الطبيعي أن نسأل: أي من العمليتين يجب أن نتخذها أساسًا للتعريف؟

بيد أن الاختيار واضح حيث إنه عندما عرفنا الحلقة بصورتها العامة وجدنا أنها تكوِّن زمرة إبدالية بالنسبة لعملية الجمع ولم نضع قيودًا كثيرة على عملية الضرب، لذا فنحن أقل تحكمًا بها من عملية الجمع. ولهذا السبب نؤكد على عملية الجمع في الحلقة ونعطي التعريف التالي.

تعريف

*إذا كان ϕ تشاكلًا من R إلى R' فإن **نواة** ϕ (Kernel) والتي نكتبها $I(\phi)$ هي مجموعة كل العناصر a في R بحيث إن $\phi(a)=0$ حيث 0 هو العنصر الصفري للحلقة R' .*

تمهيدية (٣-٣-٢)

إذا كان ϕ تشاكلا من R إلى R' نواته $I(\phi)$ فإن

١ - $I(\phi)$ *زمرة جزئية من* R *بالنسبة لعملية الجمع*

٢ - *إذا كانت a في $I(\phi)$ و r في R فإن العنصرين ar و ra موجودان في $I(\phi)$.*

البرهان

بما أن ϕ هو تشاكل من R إلى R′ باعتبارهما زمرتين إبداليتين نسبة لعمليتي الجمع فيمكننا استنتاج القسم الأول من التمهيدية مباشرة من نتائجنا في نظرية الزمر.

للبرهنة على القسم الثاني إفرض أن a في $I(\phi)$ و r في R عندئذ $\phi(a)=0$

$$\phi(ar)=\phi(a)\phi(r)=0\phi(r)=0$$

حيث إن المتساوية الأخيرة هي إحدى نتائج تمهيدية (٣-٢-١). وبطريقة مشابهة نحصل على $\phi(ra)=0$. وبذلك نستنتج أنه باستعمال تعريف $I(\phi)$ فإن كلا من ar و ra موجود في $I(\phi)$ قبل الاستمرار في الشرح نوضح هذه الأفكار ببعض الأمثلة.

مثال (٣-٣-١)

لتكن R و R′ أية حلقتين ولتكن $\phi(a)=0$ لجميع العناصر a في R من البديهي أن ϕ تشاكل و $I(\phi)=R$. في هذه الحالة نسمي ϕ التشاكل الصفري (Zero-homomorphism) .

مثال (٣-٣-٢)

لتكن R حلقة و $R'=R$ ونعرف $\phi(x)=x$ لجميع العناصر x في R . من الواضح أن ϕ تشاكل وأن $I(\phi)$ تحتوي على العنصر 0 فقط.

مثال (٣-٣-٣):

لتكن $Z(\sqrt{2})$ مجموعة جميع الأعداد الحقيقية التي على الصيغة $m+n(\sqrt{2})$ حيث n,m أعداد صحيحة.

إن المجموعة $Z(\sqrt{2})$ تكون حلقة بالنسبة لعمليتي الجمع والضرب الاعتياديتين في الأعداد الحقيقية (تحقق من ذلك).

لنعرف $\phi = Z(\sqrt{2}) \to Z(\sqrt{2})$ كالتالي :

$$\phi(m+n\sqrt{2}) = m - n\sqrt{2}$$

التطبيق ϕ هو تشاكل من $Z(\sqrt{2})$ على $Z(\sqrt{2})$ ونواته $I(\phi)$ تحتوي على الصفر فقط (تحقق من ذلك) .

مثال (٣-٣-٤)

لتكن Z حلقة الأعداد الصحيحة و Z_n حلقة الأعداد الصحيحة قياس n . نعرف $\phi : Z \to Z_n$ بحيث إن $\phi(a)$ تساوي باقي قسمة a على n . يجب على القارىء أن يتحقق من أن ϕ هو تشاكل من Z على Z_n ونواته $I(\phi)$ تتكون من جميع مضاعفات n .

مثال (٣-٣-٥)

لتكن R مجموعة كل الدوال المتصلة الحقيقية القيم المعرفة على فترة الوحدة المغلقة . المجموعة R هي حلقة بالنسبة لعمليتي جمع وضرب الدوال الاعتياديتين حيث إن حاصل جمع وضرب دالتين مستمرتين هما دالتان متصلتان . لتكن F حلقة الأعداد الحقيقية ونعرف $\phi: R \to F$ بواسطة :

$$\phi(f(x)) = f\left(\tfrac{1}{2}\right)$$

عندئذ يكون ϕ تشاكلاً من R على F ونواة ϕ تتكون من جميع الدوال في R المنعدمة عند $x = \frac{1}{2}$.

جميع الأمثلة المعطاة هنا كانت باستخدام حلقات إبدالية . هناك العديد من الأمثلة الشيقة في حالة الحلقات غير الإبدالية ولكن من السابق لأوانه أن نناقش مثل هذه الأمثلة الآن .

تعريف

*ندعو التشاكل من R إلى R′ **تماثلاً** (isomorphism) إذا كان هذا التشاكل تطبيقاً أحاديا*

تعريف

يقال عن حلقتين أنهما متماثلتان (isomorphic) إذا وجد تماثل من إحداهما على (onto) الأخرى.

الملاحظة التي ذكرت في الفصل الثاني حول معنى التماثل وحول معنى كون زمرتين متماثلتين سارية المفعول بالنسبة للحلقات وعلى النمط نفسه وكذلك المعيار المعطى تمهيدية (٢-٧-٤) حول كون التشاكل تماثلاً يترجم من حالة الزمر إلى الحلقات بالصيغة التالية.

تمهيدية (٣-٣-٣)

يكون التشاكل ϕ من R إلى R' تماثلاً إذا وفقط إذا كان $I(\phi)=0$

(٣-٤) المثاليات والحلقات الخارجه

اعتماداً على خبرتنا السابقة في الزمر بيّنا فكرة التشاكل ونواته في الحلقات، لذا فإنه من المفيد أن نعين نظير فكرة الزمرة الجزئية الناظمية في الحلقات، وعندما ننجز ذلك فإنه من المؤمل أن يقودنا هذا النظير لتكوين بنية في الحلقات شبيهة ببنية الزمرة الخارجة لزمرة بواسطة زمرة ناظمية جزئية. أخيراً إذا كنا متفائلين فإنه من المؤمل أن جميع مبرهنات التشاكل للزمر تنتقل بأكملها إلى مبرهنات تشاكل للحلقات.

من حسن الحظ يمكننا إنجاز كل ذلك حاصلين على طرائق دقيقة لدراسة الحلقات تحليلياً.

أول ما نبدأ به الآن هو تعريف مفهوم «الزمرة الناظمية الجزئية» في حالة الحلقات.

وبالعودة لما درسناه سابقًا فإن هذا الأمر ليس صعبًا. فإذا تذكرنا أن الزمر الناظمية الجزئية ما هي إلا نوى تشاكلات بالرغم من أن تعريفها الأولي لم يتضمن ذكر التشاكلات. فلماذا لا نتستعمل هذه الملاحظة في تعريفنا بالنسبة للحلقات؟.

التمهيدية (٣-٣-٢) قد أعطتنا بعض الشروط الواجب توفرها في مجموعة جزئية من الحلقة لتكون نواة تشاكل.

الآن وحيث إنــه لا توجد معلومات أخرى متوفرة لنا، فسنجعل من استنتاج تمهيدية (٣-٣-٢) نقطة البداية في محاولتنا وبذا نحصل على التعريف التالي:

تعريف

*يقال للمجموعة الجزئية غير الخالية U من R إنها مثالي **Ideal** (ثنائي الجانب) من R إذا تحقق كل من الشرطين:*

١ - كانت U زمرة جزئية من R بالنسبة لعملية الجمع.

٢ - كان كل من ru وur في U وذلك لكل عنصر u في U وr في R.

الشرط الثاني يؤكد أن U «تمتص» الضرب من اليمين ومن اليسار بأي عنصر في الحلقة. لهذا السبب فإنه من المعتاد أن يطلق على U مثالي ثنائي الجانب. سوف ترى أنه لن تمر علينا مناسبات إلا في بعض التمارين حيث ترد مثاليّات بأوصاف خاصة، لذا فإننا سنكتفي فيما سيأتي باستعمال كلمة مثالي فقط للدلالة على المثالي ثنائي الجانب.

إذا كان U مثاليا في حلقة R ، فلتكن R/U مجموعة كل المجموعات المشاركة المختلفـة لـU في R باعتبـار U زمـرة جزئية في R بالنسبـة لعملية الجمع. لاحظ أننا استعملنا كلمة مجموعة مشاركة دون وصفها بأنها يمنى أو يسرى، هذا ممكن لأن R زمرة إبدالية بالنسبة لعملية الجمع. لنعيد ما قد ذكرناه الآن فنقول إن R/U تحتوي على المجموعات المشاركة a+U ، حيث a في R . ووَفْقًا لنتائج الفصل الثاني، R/U هي تلقائيا زمرة بالنسبة لعملية الجمع، المعرفة كما يلي:

$$(a+U) + (b+U) = (a+b)+U$$

ولكي نبني حلقة من R/U يجب علينا أن نعرف عملية ضرب في R/U ، وليس أكثر سهولة من أن نعرف

$$(a+U)(b+U) = ab + U$$

ولكن يجب أن نتحقق من أن هذا التعريف هو ذو مدلول، وبمعنى آخر أن نبرهن على أنه إذا كانت

$$a+U = a'+U$$

و

$$b+U = b'+U$$

فإنه وَفْق تعريفنا للضرب يجب أن نحصل على

$$(a+U)(b+U) = (a'+U)(b'+U)$$

وبصورة مكافئة يجب أن نبين أن

$$ab+U = a'b'+U$$

ولـكي نحقق ذلــك لاحظ أولاً أنــه لما كان $a+U=a'+U$ فإن $a=a'+u_1$ حيث u_1 في U وبصورة مشابهة $b=b'+u_2$ حيث u_2 في U ، ولذا فإن

$$ab=(a'+u_1)(b'+u_2) = a'b'+u_1b'+a'u_2+u_1u_2$$

وحــيث إن U هو مثــالي في R فإن u_1b' ، و $a'u_2$ ، u_1u_2 في U . ونستنتج من ذلك أن

$$u_1b'+a'u_2+u_1u_2=u_3\in U$$

وبالتالي فإن

$$ab=a'b'+u_3$$

ونستنتج أن

$$ab+U=a'b'+u_3+U$$

وحيث إن u_3 في U لذا فإن

$$u_3+U=U$$

والذي نخرج به من كل ما ذكر أعلاه هو أن

$$ab+U=a'b'+U$$

ونكون بذلك قد انتهينا من الخطوة الرئيسة للوصول إلى هدفنا وهو تقديم عملية ضرب حسنة التعريف. أما الباقي فهوعمل رتيب. كي نُبيِّن أن R/U هي حلقة يكفينا

أن نمر على المسلمات (axioms) المختلفة التي تعرف الحلقة ونتأكد من أنها تتحقق في R/U . كل هذه التحققات متشابهة لذا فإننا نختار إحدى المسلمات وهي قانون التوزيع من اليمين ونبرهن على أنه يتحقق في R/U . الباقي متروك للقارىء كتمارين.

لتكن $X=a+U$, $Y=b+U$, $Z=c+U$ هي ثلاثة عناصر في R/U حيث a,b,c في R عندئذ

$$(X+Y)\,Z = ((a+U) + (b+U))\,(c+U) = ((a+b)+U)\,(c+U) = (a+b)c+U$$
$$= ac+bc+U = (ac+U) + (bc+U)$$
$$= (a+U)\,(c+U) + (b+U)\,(c+U)$$
$$= XZ + YZ.$$

لقد جعلنا من R/U حلقة ومن الواضح أنه إذا كانت R إبدالية فكذلك R/U لأن

$$(a+U)(b+U) = ab+U = ba+U = (b+U)\,(a+U)$$

(عكس هذا غير صحيح).

إذا كان للحلقة R عنصر وحدة 1 فإن لـ R/U عنصر الوحدة $1+U$. يمكن أن نسأل ما علاقة R/U بالحلقة R ؟

من الخبرة التي لدينا الآن، فإن من السهل الإجابة على هذا السؤال. يوجد تشاكل ϕ من R على R/U معرف بـ $\phi(a)=a+U$ لكل a في R ونواته هي بالتحديد U (يجب على القارىء أن يتحقق من أن ϕ بتعريفه أعلاه هو تشاكل من R على R/U ونواته U).

نلخص هذه الملاحظات في الآتي:

تمهيدية (٣-٤-١)

إذا كان U مثاليا في الحلقة R فإن R/U هي حلقة كما أنها صورة تشاكلية للحلقة R .

والآن بعد أن أنجزنا بنجاح عملية بناء حلقة خارجة (quotient ring) لحلقة بواسطة مثالي فيها نكون قادرين على تقديم مبرهنات التشاكل في الحلقات المشابهة لمثيلاتها في الزمر. وحيث إن براهين هذه المبرهنات في حالة الحلقات مشابهة تمامًا للبراهين في الزمر فإننا ندعو القارىء للعودة إلى الفصل الثاني من هذا الكتاب لاستذكار تلك البراهين ونكتفي هنا بسرد المبرهنة التالية.

مبرهنة (٣-٤-١)

لتكن R',R حلقتين و ϕ تشاكلًا من R على R' نواته U . عندئذ تكون الحلقة R' مماثلة للحلقة R/U وفضلًا عن ذلك، يوجد تقابل بين مجموعة المثاليات في R' ومجموعة المثاليات في R التي تحتوي U . هذا التقابل يربط كل مثالي W' في R' بالمثالي W في R المعرف وَفْق ما يلي:

$$W= \{x\in R \mid \phi(x)\in W'\}$$

مع هذا التعريف للمثالي W فإن R/W تماثل R'/W' .

مسائل

١ - إذا كان U مثاليا في R و 1 في U . فبرهن على أن $U=R$

٢ - إذا كان F حقلًا. فبرهن على أن F لا يحتوي مثاليات ما عدا (0) و F نفسها.

٣ - برهن على أن أي تشاكل من حقل هو إما تماثل أو أنه يأخذ كل عنصر إلى الصفر.

٤ - لتكن R حلقة إبدالية و a في R.

(أ) بين أن $aR=\{ar \mid r\in R\}$ هو مثالي ثنائي الجانب في R .

(ب) بيّن بمثال أن هذا يمكن أن يكون خطأً إذا لم تكن R إبدالية.

٥ - إذا كان U و V مثاليين في R وكان $U+V=\{u+v \mid u\in U, v\in V\}$
فبرهن على أن $U+V$ هو كذلك مثالي في R

٦ - إذا كان U و V مثاليين في R وكانت UV مجموعة جميع العناصر التي يمكن كتابتها على هيئة حواصل جمع منتهية لعناصر من الصيغة uv حيث u في U و v في V .
فبرهن على أن UV مثالي في R .

٧ - في تمرين ٦ برهن على أن $UV \subset U \cap V$

٨ - إذا كانت R هي حلقة الأعداد الصحيحة وكان U هو المثالي الذي يحتوي على جميع مضاعفات العدد 17 . فبرهن على أنه إذا كان V مثالي في R و $R \supset V \supset U$ فإنه إما $V=R$ أو $V=U$. عمم الفكرة!

٩ - إذا كان U مثاليا في R وكانت $r(U)=\{x \in R | xu=0$ لجميع $u \in U\}$
فبرهن على أن $r(U)$ مثالي في R .

١٠ - إذا كان U مثاليا في R وكانت $[R:U] = \{x \in R | rx \in U$ لجميع $r \in R\}$
فبرهن على أن المجموعة $[R:U]$ مثالي في R وأنها تحتوي U

١١ - لتكن R حلقة بعنصر وحدة . باستعمال عناصر الحلقة R نعرف حلقة أخرى $\bar{R}$ وذلك بتعريف $a \oplus b=a+b+1$ و $a.b=ab+a+b$
حيث a,b في R وحيث إن عمليتي الجمع والضرب في الجانب الأيمن من هاتين العلاقتين هما عمليتا الحلقة R

(ا) برهن على أن $\bar{R}$ حلقة بالنسبة للعمليتين $\oplus$ و . .

(ب) ما هو العنصر الذي يعمل عمل العنصر الصفري في $\bar{R}$ ؟

(جـ) ما هو العنصر الذي يعمل عمل عنصر الوحدة في $\bar{R}$ ؟

(د) برهن على أن R مماثلة للحلقة $\bar{R}$

١٢* - في المثال (٣-١-٦) ناقشنا حلقة المصفوفات من نوع 2×2 على الأعداد النسبية . برهن على أن الحلقة لا تحوي مثاليات عدا (0) والحلقة نفسها .

١٣* - في المثال (٣-١-٨) ناقشنا الرباعيات الحقيقية . باستخدام ذلك المثال كنموذج تعرف الرباعيات على الأعداد الصحيحة قياس p ، حيث p عدد أولي فردي ، باستخدام الطريقة ذاتها ولكن الآن باعتبار جمع الرموز التي على الصيغة

$$\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$$

حيث $\alpha_3, \alpha_2, \alpha_1, \alpha_0,$ أعداد صحيحة قياس p

(ا) برهن على أن هذه حلقة تحوي p^4 من العناصر ولا تحتوي على مثاليات سوى (0) والحلقة ذاتها

(ب)** برهن على أن هذه الحلقة ليست حلقة قسمة.

إذا كانت R أية حلقة فيقال لمجموعة جزئية L في R مثالي أيسر في R إذا تحقق ما يلي:

(١) L زمرة جزئية من R بالنسبة لعملية الجمع

(٢) لكل عنصر r في R و a في L يكون حاصل الضرب ra في L

(وبصورة مشابهة يمكن تعريف المثالي الأيمن). ولذلك فالمثالي هو في الوقت نفسه مثالي أيمن وأيسر.

١٤ - إذا كان a في R وكان $Ra=\{xa|x\in R\}$ فبرهن على أن Ra هو مثالي أيسر في R

١٥ - برهن على أن تقاطع مثاليين أيسرين في R هو مثالي أيسر في R

١٦ - ماذا يمكن أن نقول عن تقاطع مثالي أيسر مع مثالي أيمن في R ؟

١٧ - إذا كانت R حلقة و a في R وكانت $r(a)=\{x\in R|ax=0\}$ فبرهن على أن r(a) هي مثالي أيمن في R

١٨ - إذا كانت R حلقة و L مثالي أيسر في R وكانت

$\lambda(L)=\{x\in R|xa=0$ لجميع $a\in L\}$

فبرهن على أن $\lambda(L)$ هي مثالي ثنائي الجانب في R .

١٩* - لتكن R حلقة فيها $x^3=x$ لجميع العناصر x في R . برهن على أن R حلقة إبدالية.

٢٠ - إذا كانت R حلقة بعنصر الوحدة 1 و ϕ تشاكلاً من R على R' . فبرهن على أن $\phi(1)$ هو عنصر الوحدة في R' .

٢١ - إذا كانت R حلقة بعنصر الوحدة 1 و ϕ تشاكلاً من R إلى حلقة تامة R' بحيث أن $I(\phi)\neq R$. فبرهن على أن $\phi(1)$ هو عنصر الوحدة في R' .

(٣-٥) مزيدٌ من المثاليات والحلقات الخارجة

نستمر هنا في دراستنا للمثاليات والحلقات الخارجة.

دعنا نتبنى، في هذه الموقع على الأقل، وجهة النظر بأن الحقل هو أكثر ما نرغب فيه من أنواع الحلقات، وربما يسأل سائل لماذا؟ قد يكون الجواب أنه

بمقدورنا أن نجري عملية القسمة في الحقل، ولذا فإن العمليات والنتائج في الحقل أكثر قربا من تجربتنا مع الأعداد الحقيقية والمركبة.

بالإضافة إلى ذلك فكما بُيِّنَ في المسألة الثانية في مجموعة المسائل السابقة، أنه ليس للحقل صورة تشاكلية عدا الحقل نفسه أو الحلقة التافهة الحاوية على الصفر فقط. ولذلك لا يمكننا تبسيط الحقل بواسطة تشاكل عليه. بأخْذنا هذه الملاحظات بعين الاعتبار فإنه من الطبيعي أن نحاول ربط الحلقة العامة، بطريقة ما، مع الحقول.

ونسأل ماذا يمكن أن يتطلبه هذا الربط؟ إن المتوفر لدينا هي التشاكلات، المثاليات والحلقات الخارجة ومن هذه الأفكار سوف نصيغ هذا الربط. إن أول ما يجب عمله هو صياغة ملاحظات الفقرة السابقة بصورة دقيقة. والآن نسأل السؤال المحدد: تحت أي شروط تكون الصورة التشاكلية لحلقة حقلاً؟

سنعطي جوابا كاملا في هذا البند للحلقات الإبدالية ولكي نعالج هذا السؤال فمن الضروري أن ننظر إلى عكس نتيجة المسألة الثانية الواردة في قائمة المسائل في نهاية البند (٣-٤).

تمهيدية (٣-٥-١)

لتكن R حلقة إبدالية بعنصر وحدة والتي مثالياتها هي فقط (0) و R نفسها، عندئذ تكون R حقلاً.

البرهان

كي نبرهن على هذه التمهيدية يجب أن نوجد لكل عنصر $a \neq 0$ في R عنصراً $b \neq 0$ في R بحيث أن $ab=1$.

لذا افرض أن $a \neq 0$ في R. لنعتبر المجموعة

$$Ra=\{xa \mid x \in R\}$$

إننـا ندعي أن Ra هي مثـالي في R ولكي نحقق ذلك يجب أن نبين أنها زمرة جزئـية من R بالـنسبـة لعملية الجمـع وأنـه إذا كان u في Ra وr في R فإن ru هو كذلـك في Ra (يكفينـا أن نتـأكـد من أن ru في Ra لأنه حينئذ يكون ur في Ra لأن ru=ur) .

والآن إذا كان u ، v في Ra فإن $u=r_1a$ ، $v=r_2a$ لعـنصرين r_2 ، r_1 في R . ولذا فإن

$$u+v=r_1a+r_2a=(r_1+r_2)a\in Ra$$

وبصورة مشابهة

$$-u=-r_1a=(-r_1)a\in Ra$$

وبالتالي فإن Ra زمرة جزئية جمعية في الحلقة R . علاوة على ذلك إذا كان r في R، فإن

$$ru=r(r_1a)=(rr_1)a\in Ra$$

إذن Ra تحقق جميع شروط المثـالي في R (لاحظ أن قانوني التوزيع والتجميع لعملية الضرب قد أُسْتَعْمِلا لبرهنة هذه الحقيقة) .

ومن الفرض نجد أن $Ra=(0)$ أو $Ra=R$. ولما كان

$$0\neq a=1a\in Ra$$

فإن $Ra\neq(0)$ وبذا تتبقى لدينا الإمكانية الوحيدة الأخرى، ألا وهي $Ra=R$.

إن المـعـادلـة الأخـيرة تنص على أن أي عنصر في R هو حاصـل ضرب العنصر a بعنصر من R . وبصـورة خاصة $1\in R$ وبذلك يمكن أن نكتبه على شكل مضاعف للعنصر a ، أي يوجد عنصر b في R بحيث أن $ba=1$ وبهذا يتم برهان التمهيدية .

تعريف

*يُدعى المثالي M في حلقة R حيث $M\neq R$ **مثاليًا أعظمياً** (maximal ideal) للحلقة R في حالة أنه لكل مثالي U في R حيث $M\subset U\subset R$ إما أن يكون $R=U$ أو $M=U$.*

وبعبارة أخرى يكون مثالي في R مثاليًا أعظميًا إذا تعذر إيجاد مثالي بينه وبين الحلقة بأكملها. إذا أعطينا حلقة R فليس هناك ما يضمن وجود أي مثالي أعظمي فيها! . ولكن إذا كان للحلقة عنصر وحدة فمن الممكن البرهنة على وجود مثل هذا المثالي وذلك باستعمال إحدى المسلمات (axioms) الأساسية في الرياضيات، ألا وهي مسلمة الاختيار. كذلك يمكن أن تحوي الحلقة أكثر من مثالي أعظمي فيها، وسنبين ذلك أدناه في حلقة الأعداد الصحيحة.

إلى هذا الحد نكون قد تعرفنا على القليل من الحلقات. . وبدراستنا لفكرة ما في العديد من الحالات الخاصة يمكننا أن نعي تمامًا هذه الفكرة ودوافعها. وعلى ذلك فقبل أن نمضي في دراستنا نختبر بعض المثاليات العظمى في حلقتين معينتين. وعندما نأتي إلى الحديث عن حلقات كثيرات الحدود سوف نعرض جميع المثاليات العظمى فيها.

مثال (٣-٥-١)

لتكن R حلقة الأعداد الصحيحة، ولتكن U مثاليا في R . ولما كانت U زمرة جزئية من R بالنسبة لعملية الجمع فمن نتائجنا في نظرية الزمر نعرف أن U تحوي جميع المضاعفات لعدد صحيح محدد n_0 ونكتب هذا بالشكل $U=(n_0)$. ونسأل الآن أي القيم لعدد n_0 تجعل U مثاليًا أعظميًا؟

أولا : نزعم بأنه إذا كان p عددًا أوليًا فإن $P=(p)$ مثالي أعظمي في R . فإذا كان U مثاليًا في R، $U \supset P$ فإن $U=(n_0)$ لعدد صحيح n_0 . ولما كان $P \subset U, p \in P$ فإن $p=mn_0$ لعدد صحيح m وحيث إن p عدد أولي نستنتج أن $n_0=1$ أو $n_0=p$. إذا كان $n_0=p$ فإن $P \subset U=(n_0) \subset P$ وهذا مع $P \subset U$ يعطينا $P=U$. أما في حالة كون $n_0=1$ فإن $1 \in U$ وبالتالي $r=1r \in U$ لجميع العناصر $r \in R$ مما يؤدي إلى أن $U=R$. وبذلك لا يوجد أي مثالي بين P و R سوى R و P نفسيهما ومنه نستنتج أن P مثالي أعظمي.

ومن جهة أخرى لنفرض أن $M=(n_0)$ مثالي أعظمي في R .

إننا ندعي أن n_0 يجب أن يكون عدداً أوليًا، فلو كان $n_0=ab$ حيث b,a عددان صحيحان موجبان فإن $U=(a) \supset M$ وبذلك يكون $U=R$ أو $U=M$. إذا كان $U=R$

فمن السهل الاستنتاج أن $a=1$. وإذا كان $U=M$ فإن $a\in M$ وبذلك تكون $a=rn_0$ لعدد صحيح r ذلك لأن جميع عناصر M هي مضاعفات العدد n_0 . ولكن حينئذ يكون $a=rab$ ومن هذا نجد أن $rb=1$ مما يؤدي إلى أن $n_0=a, b=1$. وهكذا يكون n_0 عددًا أوليًا.

في هذاا المثال بالذات تبدو فكرة المثالي الأعظمي ملموسة ـ فهي تقابل بالضبط فكرة الأعداد الأولية ـ بيد أنه يجب علينا ألا نتعجل الأمر في أي تعميم، لأن هذا النوع من التقابل عادة ليس صحيحًا في الحلقات بصفة عامة.

مثال (٣ـ٥ـ٢)

لتكن R حلقة جميع الدوال المتصلة حقيقية القيم المعرفة على فترة الوحدة المغلقة. (انظر مثال ٣ـ٣ـ٥). ولتكن

$$M=\{f(x)\in R\,|\,f(\tfrac{1}{2})=0\}$$

من المؤكد أن M مثالي في R . وأكثر من ذلك هو مثالي أعظمي في الحلقة R ، ذلك أنه إذا كان المثالي U محتويًا $U\neq M$, M ، فتوجد دالة $g(x)$ في $g(x)\notin M$,U . ولأن $g(x)\notin M$ نستنتج أن $g(\frac{1}{2})=\alpha\neq 0$.

الآن لنعرف $h(x)=g(x)-\alpha$

عندئذ $h(\frac{1}{2})=g(\frac{1}{2})-\alpha=0$ وبذلك تكون $h(x)\in M\subset U$.

ولكن $g(x)$ عنصر في U مما يؤدي إلى أن α التي تساوي $g(x)-h(x)$ تقع في U ومن هذا نجد أن $1=\alpha\alpha^{-1}\in U$. وهكذا فإنه لأية دالة $t(x)\in R$ تكون $t(x)=1t(x)\in U$ وبذلك نحصل على $U=R$. إذن M مثالي أعظمي في R . وبنفس الطريقة يمكننا أن نبرهن على أنه لأي عدد حقيقي γ حيث $0\leq\gamma\leq 1$ فإن $M_\gamma=\{f(x)\in R\,|\,f(\gamma)=0\}$ مثالي أعظمي في R . يمكن البرهنة (انظر مسألة ٤ في نهاية هذا البند) بأن كل مثالي أعظمي في R هو على الشاكلة أعلاه. وهكذا فإن المثاليات الأعظمية تقابل النقاط على فترة الوحدة.

وبعد أن رأينا بعض المثاليات الأعظمية في حلقات معينة نستمر في عرض المادة.

مبرهنة (٣-٥-١)

إذا كانت R حلقة إبدالية بعنصر وحدة و M مثاليًا في R ، فإن M مثالي أعظمي في R إذا وفقط إذا كانت R/M حقلاً.

البرهان

لنفرض أولاً أن M مثالي في R بحيث تكون R/M حقلاً، لما كان R/M حقلا فإن مثاليه الوحيدين هما {0} و R/M نفسه. ولكن حسب مبرهنة (٣-٤-١) يوجد تقابل بين مجموعة المثاليات في R/M ومجموعة المثاليات في R التي تحتوي M . المثالي M في R يقابل المثالي {0} في R/M بينما يقابل المثالي R في R المثالي R/M في R/M . وهكذا لا يوجد مثالي بين M و R غير المثاليين نفسيهما وبذا يكون M مثالياً أعظميًا.

ومن ناحية أخرى، إذا كان M مثاليًا أعظميًا في R فإنه بالرجوع إلى التقابل آنف الذكر نجد أن R/M لا تحوي مثاليا عدا R/M و {0} . وبالإضافة إلى ذلك R/M إبدالية وتحوي عنصر وحدة ذلك لأن R تتمتع بهاتين الخاصتين. وهكذا نكون قد استوفينا جميع شروط تمهيدية (٣-٥-١) في الحلقة R/M ، لذا يمكننا أن نستنتج من تلك التمهيدية أن R/M حقل.

في مناسبات عديدة في هذا الكتاب سوف نستعين بهذه النتيجة عند دراستنا حلقات كثيرات الحدود وفي نظرية امتداد الحقول.

مسائل

١ - لتكن R حلقة بعنصر وحدة، ليس من الضروري أن تكون R إبدالية، بحيث إن المثالين الأيمنين الوحيدين فيها هما {0} و R . برهن على أن R حلقة قسمة.

٢* - لتكن R حلقة بحيث أن مثالييها الأيمنين الوحيدين هما {0} و R . برهن على أنه إما أن تكون R حلقة قسمة أو حلقة تحوي عددًا أوليًا من العناصر وفيها ab=0 لجميع العناصر a و b في R .

٣ ـ لتكن Z حلقة الأعداد الصحيحة و p عددًا أوليًا و (p) المثالي الحاوي على مضاعفات p . برهن على:

(أ) أن الحلقة $Z/(p)$ تماثل Z_p حلقة الأعداد الصحيحة قياس p .

(ب) أن Z_p حقل باستعمال المبرهنة ٣ـ٥ـ١ والجزء (أ) من هذه المسألة.

٤** ـ لتكن R حلقة جميع الدوال المتصلة حقيقية القيم المعرفة على فترة الوحدة المغلقة. إذا كان M مثاليا أعظميًا في R . فبرهن على أنه يوجد عدد حقيقي γ, $0\leq\gamma\leq1$ بحيث إن

$$M=M_{\gamma}=\{f(x)\in R\mid f(\gamma)=0\}$$

(٣ـ٦) حقل خوارج القسمة للحلقة التامة

دعنا نعيد إلى الذاكرة أن الحلقة التامة هي حلقة إبدالية D لا تحوي قواسمًا للصفر أي أنه إذا كان $ab=0$ لعناصر a,b في D فإن $a=0$ أو $b=0$. تعتبر حلقة الأعداد الصحيحة مثالاً قياسيًا للحلقات التامة.

إن حلقة الأعداد الصحيحة تتمتع بصفة مهمة ألا وهي إمكانية توسيعها إلى مجموعة الأعداد النسبية التي تشكل حقلاً. ونسأل: هل بإمكاننا عمل الشيء ذاته لأية حلقة تامة؟ فيما سيأتي أدناه سنبين أن هذا الأمر ممكن حقًا.

تعريف

يقال إنه بالإمكان أن ندخل (imbed) حلقة R في حلقة R' إذا وُجد تماثل من R إلى R' . (إذا احتوت R على عنصر الوحدة 1 و R' على عنصر الوحدة $1'$ فيجب التأكيد في هذه الحالة على أن يأخذ التماثل هذا العنصر 1 إلى $1'$).

سندعو R' **حلقة فوقية** (over-ring) أو امتدادًا (extension) للحلقة R إذا أمكن إدخال R في R' . بهذا المفهوم لفكرة الإدخال نبرهن على ما يلي.

مبرهنة (٣-٦-١)

يمكن إدخال أية حلقة تامة في حقل.

البرهان

قبل أن نبدأ بتفاصيل البرهان نعطي أنفسنا بعض الحرية في التفكير في حل هذه المسألة. فلتكن D حلقتنا التامة. إن الحقل الذي ننشده عامة عبارة عن جميع خوارج القسمة a/b حيث b,a في D و $b\neq0$.

في الحلقة D قد لا يكون هناك معنى لخارج القسمة a/b . إذن ماهي متطلباتنا في هذه الرموز a/b ؟ واضح أنه يجب أن نجيب على الأسئلة الثلاثة التالية:

١ ـ متى يكون $a/b = c/d$ ؟

٢ ـ ما هو $(a/b) + (c/d)$ ؟

٣ ـ ما هو $(a/b)(c/d)$ ؟

في جوابنا على السؤال الأول نقول إنه من الطبيعي أن نجعل $a/b=c/d$ إذا وفقط إذا كان $ad=bc$.

أما بالنسبة للسؤالين الثاني والثالث فليس أوضح من أن نجعل

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd} \quad و \quad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bc}$$

في الحقيقة سنجعل من هذه الاعتبارات دليلاً لنا فيما سيأتي. لهذا دعنا نترك طريقة التحري ولندخل في مجال الرياضيات بتقديم التعاريف والاستنتاجات الدقيقة.

لتكن **M** مجموعة الأزواج المرتبة (a,b) حيث b,a في D و $b\neq0$ (فكر في (a,b) وكأنها (a/b)).

نعرف في **M** العلاقة التالية:

$$(a,b)\sim(c,d) \text{ إذا وفقط إذا كان } ad=bc$$

إننا ندعي أن هذه العلاقة هي علاقة تكافؤ على **M** . كي نبين صحة ادعائنا يجب التأكد من استيفاء هذه العلاقة للشروط الثلاثة في علاقة التكافؤ وهي:

١ - إذا كان (a,b) في M فإن $(a,b)\sim(a,b)$ لأن $ab=ba$

٢ - إذا كان (a,b) و (c,d) في M وكان $(a,b)\sim(c,d)$ فإن $ad=bc$ وعليه يكون $cb=da$ مما يؤدي إلى أن $(c,d)\sim(a,b)$

٣ - إذا كان $(e,f),(c,d),(a,b)$ في M وكان $(a,b)\sim(c,d)$, $(c,d)\sim(e,f)$ فإن $cf=de$, $ad=bc$. بذا يكون $bcf=bde$ وحيث إن $bc=ad$ نستنتج أن $adf=bde$. وحيث إن D إبدالية يكون لدينا $afd=bed$ ولما كانت D حلقة تامة و $d\neq0$ فإنه ينتج من ذلك أن $af=be$ مما يؤدي إلى أن $(a,b)\sim(e,f)$ وتكون العلاقة متعدية.

الآن دع $[a,b]$ يرمز إلى فصل التكافؤ الحاوي على العنصر (a,b) ولنرمز بالحرف F لمجموعة فصول التكافؤ $[a,b]$ حيث b,a في D, $b\neq0$. هذه المجموعة F هي مرشحنا للحقل الذي ننشده. كي نجعل من F حقلاً يجب أن نعرّف عليه عمليتي جمع وضرب ثم نبين أن هاتين العمليتين تحققان شروط الحقل.

أولاً : نبدأ بعملية الجمع مسترشدين بما تحريناه في بداية البرهان فنعرف

$$[a,b]+[c,d] = [ad+bc, bd]$$

لما كانت D حلقة تامة و $d\neq0$, $b\neq0$ فإن $bd\neq0$ مما يجعل العنصر $[ad+bc, bd]$ في F . الآن نزعم أن عملية الجمع هذه حسنة التعريف، بمعنى أنه إذا كانت $[a,b]=[a',b']$, $[c,d]=[c',d']$ فإن $[a,b]+[c,d]=[a',b']+[c',d']$.

ولكي نرى ذلك لاحظ أن $[a,b]=[a',b']$ تعطينا $ab'=ba'$ وأن $[c,d]=[c',d']$ تعطينا $cd'=dc'$. الواجب علينا استعمال هذه العلاقات لتبيان أن $[a,b]+[c,d] = [a',b']+[c',d']$.

وبالرجوع إلى تعريف عملية الجمع، نجد أننا يجب أن نبرهن على أن $[ad+bc,bd]=[a'd'+b'c',b'd']$.

أو بصـــورة مكـــافئـــة أن $(ad+bc)b'd'=bd(a'd'+b'c')$. واســـتـــنـــاداً إلى أن $ab'=ba'$ و $cd'=dc'$ نحصل على:

$$(ad+bc)b'd'= adb'd'+bcb'd = ab'dd'+bb'cd'$$
$$= ba'dd'+bb'dc' = bd (a'd'+b'c')$$

والمتساوية الأخيرة هي التي كنا ننشدها.

من الواضح أن $[0,b]$ يقوم مقام العنصر الصفري في عملية الجمع و $[-a,b]$ هو المعكوس الجمعي للعنصر $[a,b]$. ومن السهل التحقق من أن F زمرة إبدالية بالنسبة لعملية الجمع.

الآن نتـولى عملية الضرب في F . هنـا أيضـا نستفيد مما ذكـرنـاه آنفـا في الـبرهـان فنعـرف $[a,b][c,d]$ على أنـه $[ac,bd]$. كما هي الحـال في عملية الجمـع هنـا أيضـا $bd\neq0$ لأن $b\neq0$ و $d\neq0$ مما يجعـل $[ac,bd]$ في F . باتـبـاعـنـا خطوات مشـابهـة لما عرضناه في عملية الجمع يمكن البرهنة على أنـه إذا كان $[a,b]=[a',b']$, $[c,d]=[c',d']$ فإن $[a,b][c,d]=[a',b'][c',d']$

في الحقيقة أنه بالإمكان البرهنة على أن العناصر غير الصفرية في F (أي جميع العناصر $[a,b]$ حيث $a\neq0$) تكون زمرة إبدالية بالنسبة لعملية الضرب وعنصر الوحدة فيها هو $[d,d]$, $[c,d]^{-1}=[d,c]$ (إن العنصر $[d,c]$ ينتمي إلى F وذلك لأن $c\neq0$).

إن التحقق من تمتع F بخاصية توزيع الضرب على الجمع أمر رتيب نتركه للقارىء.

كل ما بقي علينا الآن هو تبيان إمكانية إدخال D في F . ولأجل ذلك سنقدم تماثـلا محددًا من D إلى F . وقبـل أن نعمـل هذا لاحظ أولاً أنـه للعنصرين: $y\neq0$, $x\neq0$ في D يكـون $[ax,x]=[ay,y]$ لأن $(ax)y=x(ay)$ ، لنـرمـز للعـنـصر $[ax,x]$ بالعنصر $[a,1]$.

الآن عرف $\phi:D\to F$ على النحو $\phi(a)=[a;1]$ لكل عنصر a في D . نترك للقارىء مهمة التحقق من أن ϕ تماثـل من D إلى F وأنـه إذا كانت D تحتـوي على عنصر وحدة 1 فإن $\phi(1)$ هو عنصر الوحدة في F . بذلك نكون قد أتممنا برهان المبرهنة.

يطلق على الحقل F **حقل خوارج القسمة** (field of quotients) للحلقة التامة D . في حالة كون D حلقة الأعداد الصحيحة يكون الحقل F بطبعية الحال حقل الأعداد النسبية .

مسائل

١ ـ برهن على أنه إذا كان

$$[c,d]=[c',d'], \quad [a,b]=[a',b']$$

فإن

$$[a,b][c,d]=[a',b'][c',d']$$

٢ ـ برهن قانون التوزيع في F .

٣ ـ برهن على أن التطبيق $\phi = D \rightarrow F$ المعرف على النحو $\phi(a)=[a,1]$ هو تماثل من D إلى F .

٤ ـ برهن على أنه إذا كان K حقلاً ما يحوي D فإن K يحوي حقلاً جزئيًا مماثلاً للحقل F . (*بهذا المعنى نعتبر F أصغر حقل يحوي D*) .

*٥ ـ لتكن R حلقة إبدالية بعنصر وحدة. تدعى المجموعة الجزئية غير الخالية S في R نظامًا ضربياً إذا

- ـ كانت المجموعة غير حاوية على العنصر الصفري .
- ـ كان العنصران s_1 و s_2 في S فيجب أن يكون s_1s_2 في S .

لتكن **M** مجموعة الأزواج المرتبة (r,s) حيث r في R و s في S .

في **M** عرف العلاقة $(r,s)\sim(r',s')$ إذا وفقط إذا وجد عنصر s'' في S بحيث إن

$$s''(rs'-sr')=0$$

(ا) برهن على أن العلاقة أعلاه هي علاقة تكافؤ على **M** .

لنرمز إلى فصل التكافؤ للعنصر (r,s) بالرمز [r,s] ولتكن R_s مجموعة فصول التكافؤ. في R_s عرف

$$[r_1,s_1]+[r_2,s_2] = [r_1s_2+r_2s_1,s_1s_2]$$

و

$$[r_1,s_1][r_2,s_2]=[r_1r_2,s_1s_2]$$

(ب) برهن على أن عمليتي الجمع والضرب أعلاه حسنتا التعريف وأن R_s حلقة بالنسبة إلى هاتين العمليتين.

(جـ) هل بالإمكان إدخال R في R_s ؟

(د) برهن على أن التطبيق $\phi:R\to R_s$ المعرّف على النحو $\phi(a)=[as,s]$ هو تشاكل من R إلى R_s ثم أوجد نواة ϕ .

(هـ) برهن على أن هذه النواة لا تحوي عنصرًا من S .

(و) برهن على أن أي عنصر على الصيغة $[s_1,s_2]$ (حيث s_2,s_1 في S) في R_s له معكوس ضربي في R_s .

٦ ـ لتكن D حلقة تامة و b,a عنصرين في D . نفرض أن $a^n=b^n$ و $a^m=b^m$ حيث m,n عددان صحيحان موجبان أوليان نسبياً. برهن على أن $a=b$.

٧ ـ لتكن R حلقة، قد تكون غير إبدالية، وفيها $xy=0$ تقتضي أن $x=0$ أو $y=0$. إذا كان b,a في R وكان $a^n=b^n$ و $a^m=b^m$ حيث m,n عددان صحيحان موجبان أوليان نسبيًا، فبرهن على أن $a=b$.

(٣-٧) الحلقات الإقليدية

إن ما يقودنا إلى دراسة نوع الحلقات في هذا البند هو وجود العديد من الأمثلة الحية عليها مثل حلقة الأعداد الصحيحة، أعداد جاوس الصحيحة (Gaussian integers) (بند ٣ ـ ٨) وحلقات كثيرات الحدود (Polynomial rings) (البند ٣-٩). إن تعريف هذا النوع من الحلقات مصمم ليشتمل على الخواص المميزة للحلقات الثلاثة المذكورة أعلاه.

تعريف

*يُطلَق على الحلقة التامة R إسم **حلقة إقليدية** (Euclidean ring) إذا كان لأي عنصر $a\neq 0$ في R يوجد عدد صحيح غير سالب $d(a)$ بحيث إنه*

١ - لجميع b,a في R ، كلاهما غير صفري يكون $d(a)\leq d(ab)$.
٢ - لأي عنصرين b,a في R ، كلاهما غير صفري ، يوجد عنصران r,t في R بحيث إن $a=tb+r$ حيث $r=0$ أو $d(r)<d(b)$.

لاحظ أننا لم نعرف $d(0)$. إن حلقة الأعداد الصحيحة هي مثالنا الأول على الحلقات الإقليدية حيث $d(a)$ تساوي القيمة المطلقة للعدد a . في البند القادم سنرى أن أعداد جاوس الصحيحة هي مثال آخر على الحلقة الإقليدية . ومن هذه الملاحظة ونتائج سنثبتها في هذا البند سوف نبرهن إحدى المبرهنات العريقة في نظرية الأعداد المنسوبة إلى فرما (Fermat) ، ألا وهي أن أي عدد أولي على الصيغة $4n+1$ يمكن كتابته كحاصل جمع مربعين.

نبدأ موضوعنا بما يلي :

مبرهنة (٣-٧-١)

لتكن R حلقة إقليدية و A مثالي في R ، عندئذ يوجد عنصر a_0 في A بحيث إن A تحوي بالضبط جميع العناصر على الصيغة a_0x حيث x في R .

البرهان

إذا احتوت A على العنصر 0 فقط فضع $a_0=0$ وتكون المبرهنة صحيحة في هذه الحالة . وهكذا يمكننا الفرض أن $A\neq\{0\}$ وبذلك يوجد عنصر $a\neq0$ في A . اختر a_0 في A بحيث إن $d(a_0)$ هو أصغر ما يمكن . (يمكننا عمل ذلك لأن d يأخذ قيمًا صحيحة غير سالبة) .

نفرض أن a في A فبالرجوع إلى خواص الحلقات الإقليدية يمكننا إيجاد عنصرين t و r في R بحيث إن $a=ta_0+r$ حيث $r=0$ أو $d(r)<d(a_0)$. لما كان a_0 في A و A مثالي في R فإن ta_0 في A مما يؤدي إلى أن $a-ta_0$ في A ولكن $r=a-ta_0$ لذا فإن r في A . إذا كان $r\neq0$ فإن $d(r)<d(a_0)$

مما يعطينا عنصرًا r في A تكون قيمة الدالة d له أصغر من قيمتها للعنصر a_0 وهذا يناقض اختيارنا للعنصر a_0 في A . ونتيجة لذلك يجب أن يكون $r=0$ و $a=ta_0$ مما يثبت المبرهنة.

فيما سيأتي سنستعمل الرمز (a) ليرمز إلى المثالي $\{xa|x\in R\}$ الحاوي على جميع مضاعفات a .

تعريف

يطلق على الحلقة التامة R بعنصر وحدة إسم ***حلقة رئيسة المثالي*** *(Principal ideal ring) إذا كان أي مثالي A في R هو من الصيغة (a) لعنصر ما a في R .*

بالاستناد إلى المبرهنة (٣-٧-١) فإنه يكفينا أن نثبت وجود عنصر وحدة في الحلقة الاقليدية كي تكون حلقة رئيسة المثالي. وقبل أن نفعل ذلك نود أن نشير إلى أنه ليست كل حلقة رئيسة المثالي هي حلقة إقليدية (أنظر:

Motzkin, T. "The Euclidean Algorithm." *Bulletin of the American Mathematical Society*, vol.55 (1949), 1142-1146.

نتيجة

كل حلقة إقليدية تحوي عنصر وحدة.

البرهان

لتكن R حلقة إقليدية، إن R بدون شك مثالي في R ، لذا فإن $R=(u_0)$ لعنصر ما u_0 في R حسب المبرهنة (٣-٧-١). عندئذ يكون أي عنصر في R مضاعفًا للعنصر u_0. إذن، وبصفة خاصة، $u_0=u_0c$ لعنصر ما c في R . إذا كان a في R فإن $a=xu_0$ لعنصر ما x في R وبالتالي فإن $ac=(xu_0)c = x(u_0c) = xu_0=a$. هكذا نكون قد بينا أن c عنصر الوحدة المنشود.

تعريف

إذا كان $a\neq 0$ و b عنصرين في حلقة إبدالية R فيقال إن a يقسم b إذا وجد عنصر c في R بحيث أن $b=ac$. سنستعمل الرمز $a|b$ ليعني أن a نقسم b والرمز $a \nmid b$ ليعني أن a لا يقسم b .

ملاحظة

١ ـ إذا كان $a|b$ و $b|c$ فإن $a|c$.

٢ ـ إذا كان $a|b$ و $a|c$ فإن $a|(b\pm c)$.

٣ ـ إذا كان $a|b$ فإن $a|bx$ لكل x في R .

إن برهان الملاحظة أعلاه بسيط جدًا لذا قررنا حذفه.

تعريف

*إذا كان b,a في R فيقال لعنصر d في R إنه **قاسم مشترك أعظم** (greatest common divisor) للعنصرين b,a إذا*

١ ـ كان $d|a$ و $d|b$.

٢ ـ كلما كان $c|a$ و $c|b$ فإن $c|d$.

سوف نستعمل الرمز $d=(a,b)$ ليعني أن d قاسم مشترك أعظم للعنصرين b,a .

تمهيدية (٣-٧-١)

لتكن R حلقة إقليدية عندئذ لأي عنصرين b,a في R يوجد قاسم مشترك أعظم d ، وفضلا عن ذلك ، $d=\lambda a+\mu b$ حيث μ,λ عنصران في R .

البرهان

لتكن A مجموعة جميع العناصر على الشكل $ra+sb$ لجميع العناصر s,r في R . إننا ندعي أن A مثالي في R . ولإثبات ذلك نفرض y,x في A فيكون

$x=r_1a+s_1b$ و $y=r_2a+s_2b$ وبـذا يكـون $x\pm y=(r_1\pm r_2)a+(s_1\pm s_2)b$ في A . وبصورة مشابهة نرى أنه لأي عنصر u في R يكون $ux=u(r_1a+s_1b) = (ur_1)a+(us_1)b$ في A .

لما كان A مثاليًا في R فبالرجوع إلى المبرهنة (٣-٧-١) يوجد عنصر d في A بحيث كل عنصر في A هو مضاعف للعنصر d . ولكون d في A فإن $d=\lambda a+\mu b$ لعنصرين λ و μ في R . والآن نستعين بنتيجة المبرهنة (٣-٧-١) والتي تنص على أن R تحتوي على عنصر وحدة مما يؤدي إلى أن $a=1a+0b$ في A و $b=0a+1b$ في A . ينتج عن ذلك أن b,a مضاعفان للعنصر d أي أن $d|a, d|b$.

نفرض، أخيرًا، أن $c|a$ و $c|b$ ، عندئذ، $c|\lambda a$ و $c|\mu b$ مما يؤدي إلى أن c يقسم $\lambda a+\mu b$ أي $c|d$. وهكذا نرى أن d تتمتع بجميع صفات القاسم المشترك الأعظم مما يكمل برهان التمهيدية.

تعريف

لتكن R حلقة إبدالية بعنصر وحدة. يُطلق على عنصر a في R إسم وحدة unit في R إذا وجد عنصر b في R بحيث أن $ab=1$.

لا تخلط بين التسميتين **وحدة في** R و **عنصر وحدة في** R . **فالوحدة في حلقة هي** عنصر يكون معكوسها الضربي موجودًا في الحلقة.

تمهيدية (٣-٧-٢)

لتكن R حلقة تامة بعنصر وحدة وافرض أنه لعنصرين b,a في الحلقة $a|b$ و $b|a$ عندئذ $a=ub$ حيث u وحدة في R .

البرهان

لما كان $a|b$ فإن $b=xa$ لعنصر ما x في R ولما كان $b|a$ فإن $a=yb$ لعنصر

ما y في R . وهكذا يكون $b=x(yb)=(xy)b$ ولكن R حلقة تامة مما يمكننا من حذف العنصر b لنحصل على $xy=1$ أي أن y وحدة في $a=yb, R$ مما يكمل برهان التمهيدية.

تعريف

لتكن R حلقة إبدالية بعنصر وحدة. يقال عن عنصرين b,a في R إنهما ***شريكان*** *(associates) إذا كان $b=ua$ لوحدة ما u في R .*

إن علاقة المشاركة هي علاقة تكافؤ (مسألة ١ في نهاية هذا البند). كذلك لاحظ أنه في الحلقة الإقليدية كل قاسمين مشتركين أعظمين لعنصرين معينين هما عنصران شريكان (مسألة ٢).

إلى هذا الحد من دراستنا للحلقات الإقليدية لم نستعمل الشرط الأول في تعريف تلك الحلقات وهو $d(a)\leq d(ab)$ عندما $b\neq 0$. والآن فقد حان الوقت لاستعمال هذا الشرط في برهان التمهيدية التالية.

تمهيدية (٣-٧-٣)

لتكن R حلقة إقليدية و b, a في R . إذا كان $b\neq 0$ وهو ليس وحدة في R ، فإن $d(a)<d(ab)$.

البرهان

اعتبر المثالي $A=(a)=\{xa|x\in R\}$ في R .

باستعمال الشرط الأول للحلقة الإقليدية نحصل على $d(a)\leq d(xa)$ حيث $x\neq 0$ في R . وهكذا تكون قيمة d للعنصر a هي أصغر قيمة لها لجميع عناصر A .

ومن الواضح أن ab في A فلو كان $d(ab)=d(a)$ فبالعودة إلى برهان مبرهنة (٣-٧-١) نستنتج أن كل عنصر في A هو مضاعف للعنصر ab ذلك لأن قيمة d

للعنصر ab هي أصغر ما يمكن لعناصر A . وبذلك وعلى الخصوص يجب أن يكون العنصر a في A مضاعفا للعنصر ab أي أن a=abx لعنصر ما x في R . ولكننا في حلقة تامة فنحصل على bx=1 . وهكذا يكون b وحدة في R مما يناقض الفرض. وهذا يقودنا إلى أن d(a)<d(ab) .

تعريف

لتكن R حلقة إقليدية، يطلق على عنصر π إسم ***عنصر أولي*** *(prime element) في R إذا كان π ليس وحدة في R وعندما يكون π=ab حيث b,a في R ، فإنه إما أن يكون a أو b وحدة في R .*

لذا يمكن القول بأن العنصر الأولي في R هو العنصر الذي لا يمكن تحليله بصورة غير تافهة في R .

تمهيدية (٣-٧-٤)

لتكن R حلقة إقليدية، عندئذ أي عنصر في R هو إما وحدة في R أو يمكن كتابته على هيئة حاصل لضرب لعدد منته من العناصر الأولية في R .

البرهان

سيكون البرهان بالاستقراء الرياضي على d(a)

إذا كان d(a)=d(1) فإن a وحدة في R (مسألة ٣) وبذلك تكون التمهيدية صحيحة في هذه الحالة.

الآن نفرض أن d(a)>d(1) وأن التمهيدية صحيحة لجميع العناصر x في R بحيث d(x)<d(a) . نود أن نبرهن على أن هذا الفرض يجعل a محققًا لزعم التمهيدية. هذا ما سيكمل الاستقراء ويبرهن التمهيدية.

إذا كان a عنصرًا أوليًا عندئذ يتحقق استنتاج التمهيدية في هذه الحالة. لذا فلنفترض أن a=bc حيث c,b ليسا وحدتين في R . بالرجوع إلى تمهيدية **(٣-٧-٣)**

. $d(c)<d(bc)=d(a)$ و $d(b)<d(bc)=d(a)$.

وباستعمال فرضية الاستقراء يمكن كتابة العنصرين c,b على شكل حاصل ضرب عدد منتهٍ من العناصر الأولية في R أي أن $b=\pi_1\pi_1\dots\pi_n$ و $c=\pi'_1\pi'_2\dots\pi'_m$ حيث π_i ، $1\le i\le n$ و π'_j ، $1\le j\le m$ عناصر أولية في R . وكنتيجة مما سبق نحصل على $a=bc=\pi_1\pi_2\dots\pi_n\pi'_1\pi'_2\dots\pi'_m$ وبهذا يكون a قد كُتب على هيئة حاصل ضرب عناصر أولية في R مما يكمل البرهان .

تعريف

*في الحلقة الإقليدية R يقال عن عنصرين b,a في R إنهما **أوليان نسبيا** (relatively prime) إذا كان قاسمهما المشترك الأعظم وحدة في R .*

وحيث إن كل شريك لقاسم مشترك أعظم هو أيضا قاسم مشترك أعظم ولأن 1 شريك لأية وحدة فعندما يكون b,a عنصرين أوليين نسبياً يمكننا الفرض أن $(a,b)=1$.

تمهيدية (٣-٧-٥)

لتكن R حلقة إقليدية ولنفرض أنه للعناصر a ، b ، c في R ، $a|bc$ و$(a,b)=1$ عندئذ $a|c$.

البرهان:

كما رأينا في تمهيدية (٣-٧-١) فإن القاسم المشترك للعنصرين b,a يمكن كتابته على الصيغة $\lambda a+\mu b$. وهكذا وبالفرض نحصل على $\lambda a+\mu b=1$. وبضرب هذه العلاقة بالعنصر c نحصل على $\lambda ac+\mu bc=c$. والآن $a|\lambda ac$ و $a|\mu bc$ لأن $a|bc$ بالفرض . إذن $a|(\lambda ac+\mu bc)=c$ وهذا الذي نريد إثباته في التمهيدية .

بودنا أن نبين أن العناصر الأولية في الحلقة الإقليدية تلعب نفس دور الأعداد الأولية في حلقة الأعداد الصحيحة . إذا كان π عنصرًا أوليا في a,R أي عنصر في R فإنه

إما $\pi|a$ أو $(\pi,a)=1$. لأنه، وعلى الخصوص، (π,a) يقسم π لذا يجب أن يكون إما π أو 1 (أو أي وحدة). إذا كان $(\pi,a)=1$ فيكون جزء من ادعائنا صحيحًا. وإذا كان $(\pi,a)=\pi$ ، وحيث إن $(\pi,a)|a$ نستنتج أن $\pi|a$ ويكون الجزء الآخر من ادعائنا صحيحًا أيضا.

تمهيدية (٣-٧-٦)

إذا كان π عنصرًا أوليًا في حلقة إقليدية R و $\pi|ab$ حيث b,a في R فإن π يقسم أحد العنصرين a أو b على الأقل.

البرهان

لنفرض أن π لا يقسم a عندئذ $(\pi,a)=1$ باستخدام تمهيدية (٣-٧-٥) نجد أن $\pi|b$.

نتيجة

إذا كان π عنصرًا أوليًا في حلقة إقليدية R و $\pi|a_1a_2...a_n$ فإن π يقسم على الأقل أحد العناصر $a_1,a_2,\dots,a_n$.

الآن نستمر في مقارنتنا بين العناصر الأولية والأعداد الأولية فنبرهن على ما يلي.

مبرهنة (٣-٧-٢) (مبرهنة التحليل الوحيد unique factorization theorem)

لتكن R حلقة إقليدية و $a\neq o$ عنصرًا ليس وحدة في R . ولنفرض أن $a=\pi_1\pi_2\dots\pi_n=\pi'_1\pi'_2\dots\pi'_m$ حيث π_i و π'_j عناصر أولية في R . عندئذ $n=m$ وكل π_i ، $1\leq i\leq n$ شريك لأحد العناصر π'_j ، $1\leq j\leq m$ والعكس بالعكس كل π'_k شريك لأحد العناصر π_q .

البرهان

بالنظر إلى العلاقة $a=\pi_1\pi_2\dots\pi_n=\pi'_1\pi'_2\dots\pi'_m$ وإلى أن $\pi_1|\pi_1\pi_2\dots\pi_n$ نجد أن $\pi_1|\pi'_1\pi'_2\dots\pi'_m$. بالاستعانة بتمهيدية (٣-٧-٦) يجب أن يقسم π_1

أحد العناصر π'_i ولكن π_1 و π'_i عنصران أوليان في R ، إذن $\pi'_i=u_1\pi_1$ حيث u_1 وحدة في R .

وهكـذا يكـون $\pi_1\pi_2\ldots\pi_n=\pi'_1\pi'_2\ldots\pi'_m=u_1\pi_1\pi'_2\ldots\pi'_{i-1}\pi'_{i+1}\ldots\pi'_m$.
وباختزال π_1 من الطرفين نحصل على $\pi_2\ldots\pi_n=u_1\pi'_2\ldots\pi'_{i-1}\pi'_{i+1}\ldots\pi'_m$.

بإعادة ما سبق بالنسبة للعنصر π_2 فإنه بعد n من الخطوات يؤول الطرف الأيسر إلى العنصر 1 أما الطرف الأيمن فيصبح حاصل ضرب لعدد معين من π' (وهو زيادة m على n) . هذا سيحتم كون $n\leq m$ لأن العناصر π' ليست وحدات .

وبالطريقة نفسها نجد أن $m\leq n$ مما يجعل $n=m$. فيما سبق بيَّنا أيضا أن كل عنصر π_i له شريك π'_j والعكس بالعكس .

بضم تمهيدية (٣-٧-٤) ومبرهنة (٣-٧-٢) نحصل على ما يلي

إن أي عنصر غير صفري في حلقة إقليدية R إما أن يكون وحدة أو يمكن كتابته بصورة وحيدة (إلى حد علاقة المشاركة) كحاصل ضرب عناصر أولية في R .

نُنهي هذا البند بتعيين جميع المثاليات الأعظمية في الحلقة الإقليدية . ففي مبرهنة (٣-٧-١) برهنا على أن أي مثالي A في حلقة إقليدية R هو على الصيغة $A=(a_0)$ حيث $(a_0)=\{xa_0 \mid x\in R\}$. ونسأل الآن : ما هي الشروط الواجب توافرها في a_0 لتضمن أن A مثالي أعظمي في R ؟ نجيب على هذا السؤال فيما يلي

تمهيدية (٣-٧-٧)

يكون المثالي $A=(a_0)$ مثاليًا أعظمياً في الحلقة الإقليدية R إذا وفقط إذا كان a_0 عنصرًا أوليًا في R .

البرهان

أولاً نبرهن على أنه إذا كان a_0 عنصرًا ليس أوليًا فإن $A=(a_0)$ لا يكون مثاليًا أعظميًا في R . ومن أجل ذلك نفرض أن $a_0=bc$ حيث c,b في R وليس أي منهما وحدة في R . ليكن $B=(b)$ فمن الواضح أن $a_0 \in B$ مما يؤدي إلى أن $A \subset B$. نحن ندعي أن $A \neq B$ وأن $B \neq R$.

إذا كان $B=R$ فإن $1 \in B$ مما يؤدي إلى أن $1=xb$ لعنصر ما x في R وهذا يجعل b وحدة في R مما يخالف الفرض. ومن ناحية أخرى إذا كان $A=B$ فإن $b \in B=A$ ، حينئذ $b=xa_0$ لعنصر ما x في R . ولكن $a_0=bc$ مما يجعل $a_0=xca_0$ وهذا يؤدي إلى أن $xc=1$ أي أن c وحدة في R مما يناقض الفرض. إذن B لا تساوي أيًا من A أو R ولأن $A \subset B$ نستنتج أن A لا يمكن أن تكون مثاليًا أعظميًا في R .

وبالعكس، نفرض أن a_0 عنصرًا أولياً في R و U مثالي في R بحيث $A=(a_0) \subset U \subset R$. بالاستعانة بمبرهنة (٣-٧-١)، $U=(u_0)$ ولكن $a_0 \in A \subset U=(u_0)$ مما يجعل $a_0=xu_0$ لعنصر ما x في R . بيد أن a_0 عنصر أولي في R مما يؤدي إلى أنه إما x أو u_0 وحدة في R . إذا كان u_0 وحدة في R فإن $U=R$ (انظر مسألة ٥). ومن ناحية أخرى إذا كان x وحدة في R فإن x^{-1} في R والعلاقة $a_0=xu_0$ تصبح $u_0=x^{-1}a_0$ مما يجعل u_0 في A لأن A مثالي في R . هذا يقتضي أن $U \subset A$ ومع $A \subset U$ نستنتج أن $U=A$. إذن لا يوجد مثالي فعلي في R ما بين R,A . وهذا يعني أن A مثالي أعظمي في R .

مسائل

١ ـ في حلقة إبدالية بعنصر وحدة برهن على أن العلاقة a شريك b هي علاقة تكافؤ.

٢ ـ في الحلقة الإقليدية برهن على أن أي قاسمين مشتركين أعظمين لعنصرين b,a شريكان.

٣ ـ برهن على أن الشرط الضروري والكافي لكون عنصر a وحدة في حلقة إقليدية هو أن يكون $d(a)=d(1)$.

٤ - برهن على أنه في الحلقة الإقليدية يمكن إيجاد (a,b) بالطريقة التالية :

$b=q_0a+r_1$ ، حيث $d(r_1)<d(a)$

$a=q_1r_1+r_2$ ، حيث $d(r_2)<d(r_1)$

$r_1=q_2r_2+r_3$ ، حيث $d(r_3)<d(r_2)$

$\vdots \qquad \vdots$

$r_{r-1}=q_nr_n$

و $r_n=(a,b)$

٥ - برهن على أنه إذا احتوى مثالي U في حلقة R على وحدة من R فإن U=R .

٦ - برهن على أن الوحدات في الحلقة الإبدالية بعنصر وحدة تكون زمرة إبدالية .

٧ - إذا كان b,a عنصرين في حلقة إقليدية R فنعرف **مضاعفهما المشترك الأصغر** (least common multiple) على أنه عنصر c في R بحيث a|c و b|c ، وإذا كان x في R بحيث a|x و b|x ، فإن c|x . برهن على أن أي عنصرين في حلقة إقليدية R لهما مضاعف مشترك أصغر في R .

٨ - في المسألة (٧) إذا رمزنا للمضاعف المشترك الأصغر للعنصرين a و b بالرمز [a,b] فبرهن على أن [a,b]=ab/(a,b) .

(٣ - ٨) حلقة إقليدية خاصة

مما لا شك فيه أن التجريد في الرياضيات يكتسب قيمة وأهمية عند تخصيصه لمثال محدد فيكشف لنا ملامح جديدة من ذلكم المثال . ومن أجل ذلك سنخصص فكرة الحلقة الإقليدية على حلقة معينة ألا وهي حلقة أعداد جاوس الصحيحة . وبتطبيق النتائج العامة التي حصلنا عليها عند دراستنا للحلقات الإقليدية على أعداد جاوس الصحيحة نحصل على مبرهنة مهمة في الأعداد الأولية منسوبة للعالم فرما (Fermat) .

لتكن Z[i] مجموعة كل الأعداد المركبة التي على الصيغة a+bi حيث b,a أعداد صحيحة . تكون المجموعة Z[i] حلقة تامة بالنسبة إلى عمليتي جمع وضرب

الأعـداد المركبـة المعتـادتـين ويطلق على هذه الحلقـة إسم **حلقـة أعـداد جاوس الصحيحة** (ring of Gaussian integers) .

إن هدفنا الأول هو بيان أن $Z[i]$ حلقة إقليدية . ومن أجل ذلك يجب علينا أولاً أن نعرّف دالة $d(x)$ على جميع العناصر غير الصفرية في $Z[i]$ والتي تحقق ما يلي :

١ ـ إن $d(x)$ عدد صحيح غير سالب لكل $x\neq0$ في $Z[i]$.

٢ ـ $d(x)\leqslant d(xy)$ لكل $y\neq0$ في $Z[i]$.

٣ ـ لكـل عنصرين v,u في $Z[i]$ يوجـد عنصران r,t في $Z[i]$ بحـيث $v=tu+r$ حيث $r=0$ أو $d(r)<d(u)$.

سنعرف الدالة d كما يلي :

إذا كان $x=a+bi$ ، فإن $d(x)=a^2+b^2$.

إن تعـريف $d(x)$ هذا يحقق من دون شك الخـاصـة أو الحقيقـة أنـه إذا كان $x\neq0$ فإن $d(x)\geqslant1$. كما هو معـروف إنـه لأي عددين مركبـين y,x (ليسـا بالضرورة في $Z[i]$) يكـون $d(xy)=d(x)d(y)$. وإذا كان هذان الـعـددان في $Z[i]$ وكـان $y\neq0$ فإن $d(y)\geqslant1$ مما يجعل $d(x)=d(x)1\leqslant d(x)d(y)=d(xy)$ وهذا يبين أن الشرط الثاني متحقق .

بتركيز جهدنا الآن لإثبات صحة الشرط الثالث في $Z[i]$ للدالة d وسيتم هذا في برهان المبرهنة التالية :

مبرهنة (٣ـ٨ـ١)

الحلقة $Z[i]$ حلقة إقليدية .

البرهان

كما أشرنـا في شرحنـا أعـلاه يكفينـا لإثبـات مبرهنـة (٣ـ٨ـ١) إثبـات أنـه لكـل عنصرين y,x في $Z[i]$ يوجـد عنصران r,t في $Z[i]$ بحـيث $y=tx+r$ حيث $r=0$ أو $d(r)<d(x)$.

نبدأ بإثبات ذلك في حالة خاصة وهي عندما يكون y أي عنصر في $Z[i]$ ولكن x يساوي عددًا صحيحاً موجبًا n . لنفرض أن $y=a+bi$ ، باستعمال خوارزم القسمة لحلقة الأعداد الصحيحة يمكننا إيجاد عددين صحيحين موجبين v,u بحيث $a=un+u_1$, $b=vn+v_1$ حيث v_1,u_1 عددان صحيحان يحققان $|u_1|\leqslant\frac{1}{2}n$, $|v_1|\leqslant\frac{1}{2}n$. ليكن $t=u+vi$, $r=u_1+v_1i$ عندئذ

$$y=a+bi=un+u_1+(vn+v_1)i=(u+vi)n+u_1+v_1i=tn+r.$$

وحيث إن

$$d(r)=d(u_1+v_1i)=u_1^2+v_1^2\leqslant\frac{n^2}{4}+\frac{n^2}{4}<n^2=d(n)$$

فإننا بهذا نكون قد برهنا في هذه الحالة الخاصة على أن $y=tn+r$ حيث $r=0$ أو $d(r)<d(n)$.

الآن نعالج الحالة العامة: ليكن $y, x\neq 0$ أي عنصرين $Z[i]$ ، عندئذ يكون $x\bar{x}$ مساوياً لعدد صحيح موجب n حيث $\bar{x}$ هو المرافق للعدد المركب x . باستخدام ما أثبتناه في الفقرة أعلاه بالنسبة للعنصرين $n, y\bar{x}$ نرى أنه يوجد عنصران r,t في $Z[i]$ بحيث $y\bar{x}=tn+r$ حيث $r=0$ أو $d(r)<d(n)$. عند التعويض عن n بالعنصر $x\bar{x}$ نحصل على $d(y\bar{x}-tx\bar{x})<d(n)=d(x\bar{x})$ وباستخدام العلاقتين $d(y\bar{x}-tx\bar{x})=d(y-tx)d(\bar{x})$ و $d(x\bar{x})=d(x)d(\bar{x})$ نحصل على $d(y-tx)d(\bar{x})<d(x)d(\bar{x})$. ولكن $x\neq 0$ لذا تكون $d(\bar{x})$ عددًا موجبًا يمكن تقسيم طرفي المتباينة عليه فنحصل على $d(y-tx)<d(x)$. الآن نكتب $y=tx+r_0$ حيث $r_0=y-tx$ فتكون $r_0=0$ أو $d(r_0)=d(y-tx)<d(x)$. هكذا نكون قد أكملنا برهان هذه المبرهنة.

بعد أن برهنا على أن $Z[i]$ حلقة إقليدية أصبح بإمكاننا أن نستعين بجميع النتائج التي حصلنا عليها عند دراستنا للحلقات الإقليدية فنوظفها في دراسة الحلقة $Z[i]$.

تمهيدية (٣-٨-١)

ليكن p عدداً صحيحاً أولياً ولنفرض أنه لعدد صحيح ما c أولي بالنسبة للعدد p يمكننا إيجاد عددين صحيحين y,x بحيث $x^2+y^2=cp$ ، عندئذ يمكن كتابة p على هيئة حاصل جمع مربعي عددين صحيحين أي أنه يوجد عددان صحيحان b,a بحيث إن $p=a^2+b^2$.

البرهان

مما لا شك فيه أن حلقة الأعداد الصحيحة حلقة جزئية من Z[i] ، لنفرض أن العدد الصحيح p عنصر أولي في Z[i] . ولكن $cp=x^2+y^2=(x+yi)(x-yi)$ مما يؤدي إلى أن $p|(x+yi)$ أو $p|(x-yi)$ في Z[i] (تمهيدية ٣-٧-٦). إذا كان $p|(x+yi)$ فإن $x+yi=p(u+vi)$ مما يؤدي إلى أن $x=pu$, $y=pv$ لذا فإن p تقسم $x-yi$ أيضاً. ولكن حينئذ $p^2|(x+yi)(x-yi)=cp$ ونستنتج من هذا أن $p|c$ مما يناقض الفرض. وكذلك الحال عندما $p|(x-yi)$.

نستنتج مما سبق أن p ليس عنصراً أولياً في Z[i] وهذا يقودنا إلى أن

$$p=(a+bi)(g+di)$$

حيث $a+bi$, $g+di$ عنصران في Z[i] ليس أي منهما وحدة في Z[i] . وهذا يعني أن $a^2+b^2\neq1$, $g^2+d^2\neq1$ (انظر مسألة ٢). من $p=(a+bi)(g+di)$ نحصل على $p=(a-bi)(g-di)$ فيكون

$$p^2=(a+bi)(g+di)(a-bi)(g-di)=(a^2+b^2)(g^2+d^2).$$

إذن $(a^2+b^2)|p^2$ لذا فإن a^2+b^2 يساوي 1 و p أو p^2 ولكن $a^2+b^2\neq1$ لأن $a+bi$ ليس وحدة في Z[i] وكذلك $a^2+b^2\neq p^2$ لأنه حينئذ يكون $g^2+d^2=1$ وهذا يناقض كون $g+di$ ليس وحدة في Z[i] لذا ليس هناك مخرج سوى أن يكون $a^2+b^2=p$ مما يكمل برهان التمهيدية.

تنقسم الأعداد الأولية الفردية إلى صنفين، تلك التي تعطي باقي 1 عند تقسيمها على 4 أما الصنف الثاني فيضم الأعداد التي تعطي باقي 3 عند تقسيمها على 4 .

إن هدفنـا هو البرهان على أن أي عدد أولي من الصنف الأول يمكن كتابته كمجمـوع مربعي عددين صحيحـين بينـما لا يمكن عمل ذلك لأي عدد أولي من الصنف الثاني.

تمهيدية (٣-٨-٢)

ليكن p عدداً من الصيغة $4n+1$ ، عندئذ يمكن حل التطابق

$$x^2 \equiv -1 \mod p$$

البرهان

ليكن $x=1.2.3...(p-1)/2$. إن عدد العوامل التي كتبنا بدلالتها العدد x زوجي لأن $p-1=4n$ وينتج عن ذلك أن

$$x=(-1)(-2)(-3)...(-(\frac{p+1}{2}))$$.

ولكن $p-k \equiv -k \mod p$ لذا يكون

$$x^2 \equiv (1.2...\frac{p-1}{2})(-1)(-2)...(-(\frac{p-1}{2}))$$

$$\equiv 1.2...\frac{p-1}{2}.\frac{p+1}{2}...(p-1)$$

$$\equiv (p-1)! \equiv -1 \mod p$$

لقـد استعملنـا هنـا مبرهنـة ولسن (Wilson's Theorem) التي تقـول إن $(p-1)! \equiv -1$ قياس p (انظر مسألة ١ صفحة ١٩٢).

لتوضيح النتيجة التي حصلنا عليها نأخذ $p=13$ فيكون

$x=1.2.3.4.5.6 = 720 = 5 \mod 13$ و $5^2 \equiv -1 \mod 13$.

مبرهنة (٣-٨-٢) (فرما, Fermat)

إذا كان p عدداً أولـياً على الـشـكـل $4n+1$ ، فإن $p=a^2+b^2$ حيث b,a عددان صحيحان.

البرهان

بالاستعانة بتمهيدية (٣-٨-٢) يوجد عدد x بحيث $x^2\equiv -1 \mod p$ ، هذا العدد x يمكن اختياره بحيث إن $0\leqslant x\leqslant p-1$ لأننا لا نحتاج إلا لباقي x عند تقسيمه على p . يمكننا أيضا تصغير قيمة x أكثر لتكون $|x|\leqslant\frac{p}{2}$. ذلك لأنه إذا كان $x>\frac{p}{2}$ فإن $y=p-x$ يحقق $y^2\equiv -1 \mod p$ ، و$|y|\leqslant\frac{p}{2}$.

وبالتالي يمكننا الفرض أن لدينا عدداً صحيحاً x بحيث $|x|\leqslant\frac{p}{2}$ و x^2+1 مضاعف للعدد p ، مثلاً cp . الآن $cp=x^2+1\leqslant p^2/4+1<p^2$ لذا يكون $c<p$ مما يؤدي إلى أن $p\nmid c$. باستخدام تمهيدية(٣-٨-١) نحصل على $p=a^2+b^2$ حيث b,a عددان صحيحان مما يكمل البرهان.

مسائل

١ - أوجد جميع الوحدات في $Z[i]$.

٢ - إذا لم يكن $a+bi$ وحدة في $Z[i]$. فبرهن على أن $a^2+b^2>1$.

٣ - أوجد القاسم المشترك الأعظم في $Z[i]$ للعناصر:

(أ) $3+4i$ و $4-3i$ (ب) $11+7i$ و $18-i$

٤ - برهن على أنه إذا كان p عددًا أوليًا من الصيغة $4n+3$ فلا يمكن إيجاد عدد صحيح x بحيث $x^2\equiv -1 \mod p$.

٥ - برهن على أنه لا يوجد عدد أولي p من الصيغة $4n+3$ بحيث $p=a^2+b^2$ حيث b,a عددان صحيحان.

٦ - برهن على أنه يوجد عدد غير منته من الأعداد الأولية التي من الصيغة $4n+3$.

٧* - برهن على أنه يوجد عدد غير منته من الأعداد الأولية التي من الصيغة $4n+1$.

٨* - عين جميع العناصر الأولية في $Z[i]$.

٩* - عين جميع الأعداد الصحيحة الموجبة التي يمكن كتابتها كمجموع مربعي عددين صحيحين.

(٣-٩) حلقات كثيرات الحدود

منذ بداية تعلمنا للرياضيات وبالأحرى في المرحلة المتوسطة والثانوية تعرفنا على كثيرات الحدود. ولقد قضينا وقتا طويلا نتعلم فيه كيف نحلل كثيرات الحدود وكيف نضربها ونقسمها ونبسطها. ونود الإشارة إلى أن تحليل كثيرة حدود من الدرجة الثانية قد لاينم عن موهبة رياضية لدى الطالب.

وبعد ذلك ظهرت كثيرات الحدود في بداية دراستنا في الجامعة ولكن بنمط مختلف، ألا وهو الدوال التي تأخذ قيمة لكل عدد وكنا مهتمين بدراسة اتصالها ودراسة مشتقاتها وتكاملاتها وقيمها العظمى والصغرى.

في هذا الكتاب سوف نُعنى بدراسة كثيرات الحدود ولكن من وجهة نظر تختلف عما ذكرناه أعلاه. فبالنسبة لنا ستكون كثيرات الحدود عناصر في حلقة معيّنة وسوف نهتم بالخواص الجبرية لهذه الحلقة. وسيكون جل اهتمامنا بالحقيقة هو أن كثيرات الحدود تكون حلقة إقليدية ذات خواص ستكون فعالة في دراسة الحقول وامتداداتها.

ليكن F حقلاً، نعرف **حلقة كثيرات الحدود** (polynomial ring) في المجهول x التي نرمز لها بالرمز $F[x]$ على أنها مجموعة كل الرموز $a_0+a_1x+\dots+a_nx^n$ حيث n عدد صحيح غير سالب والمعاملات $a_0,a_1,\dots,a_n$ عناصر في الحقل F . كي تكون $F[x]$ حلقة يجب أن نحدد متى يكون عنصران من $F[x]$ متساويين وكيف نجمع ونضرب عنصرين في $F[x]$ بحيث إن جميع المسلمات الخاصة بتعريف الحلقة تتحقق في $F[x]$. وهذا سيكون هدفنا في البداية.

يمكننا تجنب التعبير «مجموعة كل الرموز» المستعمل أعلاه باستخدام فكرة المتتاليات ولكن يبدو أنه من الأفضل التعامل مع الرموز التي يألفُها أكثر القرّاء.

تعريف

إذا كانت $p(x)=a_0+a_1x+\dots+a_mx^m$، $q(x)=b_0+b_1x+\dots+b_nx^n$ كثيرتي

الحــدود في $F[x]$ ، فإن $p(x)=q(x)$ إذا وفــقط إذا كان $a_i=b_i$ لكــل عدد صحيح $i\geqslant 0$.

وهكذا نقول إن كثيرتي الحدود متساويان إذا وفقط إذا تساوت معاملاتها المتقابلة .

تعريف

إذا كان $p(x)=a_0+a_1x+\ldots+a_mx^m$، $q(x)=b_0+b_1x+\ldots+b_nx^n$ عنصرين في $F[x]$ ، فإن $p(x)+q(x)=c_0+c_1x+\ldots+c_tx^t$ حيث $c_i=a_i+b_i$ لكل i .

وبعبارة أخرى نجمع كثيرتي الحدود بجمع معاملاتها وتجميع الحدود المتشابهة . مثـلاً لجمع $1+x$ مع $3-2x+x^2$ نعتبر $1+x$ على أنه $1+x+0x^2$ ونجمع حسب القاعدة المعطاة في التعريف لنحصل على حاصل الجمع $4-x+x^2$.

يبقى لنا الآن أن نعرِّف عملية الضرب في $F[x]$ والتي تبدو أكثر تعقيداً .

تعريف

إذا كان $p(x)=a_0+a_1x+\ldots+a_mx^m$, $q(x)=b_0+b_1x+\ldots+b_nx^n$

فإن $p(x)\ q(x)=c_0+c_1x+\ldots+c_kx^k$ حيث

$c_t=a_tb_0+a_{t-1}b_1+d_{t-2}b_2+\ldots+a_0b_t$ ، ينص هذا التعريف على أن عملية ضرب كثيرتي الحـدود تتم بضرب الـرموز شكليًا وباستعمال العلاقة $x^\alpha x^\beta=x^{\alpha+\beta}$ ثم تجميع الحدود المتشابهة .

لنوضح التعريف بالمثال التالي :

لنفرض أن $p(x)=1+x-x^2$ ، $q(x)=2+x^2+x^3$

هنا $a_0=1$ ، $a_1=1$ ، $a_2=-1$ ، $a_3=a_4=\ldots=0$ ، $b_0=2$ ، $b_1=0$ ، $b_2=1$ ، $b_3=1$ ، $b_4=b_5=\ldots=0$. لذا

$$c_0=a_0b_0=1.2=2$$

$$c_1 = a_1b_0 + a_0b_1 = 1.2 + (1)(0) = 2$$

$$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = (-1)(2) + (1)(0) + (1)(1) = -1$$

$$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = (0)(2) + (-1)(0) + (1)(1) + (1)(1) = 2$$

$$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = (0)(2) + (0)(0) + (-1)(1) + (1)(1) + (1)(0) = 0$$

$$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = (0)(2) + (0)(0) + (0)(1) + (-1)(1) + (1)(0) + (0)(0) = -1$$

$$c_6 = a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6 = (0)(2) + (0)(0) + (0)(1) + (0)(1) + (-1)(0) + (1)(0) + (1)(0) = 0$$

$$C_7 = C_8 = \ldots = 0$$

إذن حسب تعريفنا يكون :

$$(1+x-x^2)(2+x^2+x^3) = c_0 + c_1x + \ldots = 2 + 2x - x^2 + 2x^3 - x^5$$

لو ضربنا كثيرتي الحدود أعلاه بالطريقة التي استعملناها في المدارس الثانوية لحصلنا على النتيجة نفسها. إن تعريفنا لحاصل الضرب هو بالأحرى نفس التعريف الذي عرفه القارىء من قبل. وبدون الخوض في أمور أخرى نزعم أن F[x] حلقة بالنسبة لهاتين العمليتين وعملية الضرب فيها إبدالية وتحتوي على عنصر وحدة. نترك التحقق من مسلمات الحلقة للقارىء.

تعريف

إذا كان $f(x)=a_0+a_1x+\ldots+a_nx^n\neq0$ و $a_n\neq0$ **فنعرف درجة** *(degree) f(x) على أنها n ونرمز لها بالرمز deg f(x) .*

لذا فإن درجة f(x) هي أكبر عدد صحيح i بحيث إن المعامل الذي ترتيبه i في f(x) لا يساوي صفرًا. إن الدرجة غير معرفة لكثيرة الحدود الصفرية. نقول إن كثير الحدود **ثابت** إذا كانت درجته صفرًا. إن دالة الدرجة المعرفة على كثيرات الحدود غير الصفرية في F[x] هي الدالة d التي نحتاجها كي نجعل من F[x] حلقة إقليدية.

تمهيدية (٣-٩-١)

إذا كان $f(x)$ و $g(x)$ عنصرين غير صفرين في $F[x]$ ، فإن

$$deg\,(f(x)g(x)) = deg\,f(x) + deg\,g(x)$$

البرهان

لنفرض أن $f(x)=a_0+a_1x+\ldots+a_mx^m$ و $g(x)=b_0+b_1x+\ldots+b_nx^n$ وأن $a_m\neq 0$ و $b_n\neq 0$. إذن $deg\,f(x)=m$ و $deg\,g(x)=n$.

بالتعريف

$f(x)g(x)=c_0+c_1x+\ldots+c_kx^k$ حيث $c_t=a_tb_0+a_{t-1}b_1+\ldots+a_1b_{t-1}+a_0b_t$.

إننــا ندعي أن $c_{m+n}=a_mb_n\neq 0$ وأن $c_i=0$ لكــل $i>m+n$. من التعــريف نجــد أن $c_{m+n}=a_mb_n$. ولــكــي نثــبــت أن $c_i=0$ لكــل $i>m+n$ لاحظ أن c_i هو حاصـل جمع حدود على الشكـل a_jb_{i-j} ، ولكن $i=j+(i-j)>m+n$ لذا إما أن يكــون $j>m$ أو $(i-j)>n$. حينئــذ يكــون a_j أو b_{i-j} مســاويًا للصــفــر مما يؤدي إلى أن $a_jb_{i-j}=0$. وحــيث إن c_i هو مجمــوع حدود مســاوية للصـفــر لذا يكــون $c_i=0$ مما يثبت ادعـاءنـا. هكـذا نجـد أن أعـلى معامل غير صفري في $f(x)g(x)$ هو c_{m+n} مما يبرهن على أن

$$deg\,(f(x)g(x))=m+n=deg\,f(x)+deg\,g(x)$$

نتيجة

إذا كان

$f(x)$ و $g(x)$ عنصرين غير صفريين في $F[x]$ فإن $deg\,f(x)\leqslant deg\,(f(x)g(x))$

البرهان

لما كان $deg\,(f(x)g(x))=deg\,f(x)+deg\,g(x)$ ، ولمــا كان $deg\,g(x)\geqslant 0$ نستنتج أن $deg\,(f(x)g(x))\geqslant deg\,f(x)$.

نتيجة

الحلقة $F[x]$ حلقة تامة

نترك برهان هذه النتيجة للقارىء.

لما كانت $F[x]$ حلقة تامة فبالاستعانة بمبرهنة (٣-٦-١) يمكن أن نكوّن لها حقل خوارج القسمة. هذا الحقل يحوي بالضبط جميع خوارج قسمة كثيرات الحدود ويسمى **حقل الدوال النسبية في x على F** .

إن الدالة $\deg f(x)$ المعرّفة لجميع $f(x)\neq 0$ في $F[x]$ تحقق ما يلي:

١ - العدد $\deg f(x)$ عدد صحيح غير سالب.

٢ - إن $\deg f(x)\leq \deg\left(f(x)g(x)\right)$ لجميع $g(x)\neq 0$ في $F[x]$.

لكي تكون $F[x]$ حلقة إقليدية مع دالة الدرجة التي تلعب دور الدالة d للحلقة الإقليدية يبقى أن نبرهن على أنه لكل $g(x),f(x)$ حيث $g(x)\neq 0$ يوجد $r(x),t(x)$ في $F[x]$ بحيث $f(x)=t(x)g(x)+r(x)$ حيث $r(x)=0$ أو $\deg r(x)<\deg g(x)$. هذا هو فحوى التمهيدية التالية.

تمهيدية (٣-٩-٢) (خوارزم القسمة Division algorithm)

لكل كثيرتي حدود $f(x)$ و $g(x)\neq 0$ في $F[x]$ يوجد كثيرتي حدود $r(x)$, $t(x)$ في $F[x]$ بحيث إن $f(x)=t(x)g(x)+r(x)$ حيث $r(x)=0$ أو $\deg r(x)<\deg g(x)$.

البرهان

في الحقيقة أن البرهان ليس إلا «عملية التقسيم الطويلة» التي استعملناها في المدرسة لتقسيم كثيرة حدود علي أخرى.

إذا كانت درجة $f(x)$ أصغر من درجة $g(x)$ فليس هناك شيء نبرهنه. ذلك إننا نجعل $r(x)=f(x)$, $t(x)=0$ فنحصل على $f(x)=0g(x)+f(x)$ حيث $\deg f(x)<\deg g(x)$ أو $f(x)=0$.

لذا فبإمكاننا الفرض أن $f(x)=a_0+a_1x+\dots+a_mx^m$ و $g(x)=b_0+b_1x+\dots+b_nx^n$ حيث $a_m\neq 0$ ، $b_n\neq 0$ ، $m\geqslant n$.

الآن دع $f_1(x)=f(x)-\frac{a_m}{b_n}x^{m-n}g(x)$ فتكون $\deg f_1(x)\leqslant m-1$. باستعمال الاستقراء الرياضي على درجة $f(x)$ يمكننا الفرض أن $f_1(x)=t_1(x)g(x)+r(x)$ حيث $r(x)=0$ أو $\deg r(x)<\deg g(x)$. ولكن حينئذ

$$f(x)-\frac{a_m}{b_n}x^{m-n}g(x)=t_1(x)g(x)+r(x)$$

مما يؤدي إلى أن

$$f(x)=\left(\frac{a_m}{b_n}x^{m-n}+t_1(x)\right)g(x)+r(x)$$

إذا جعلنا $t(x)=\frac{a_m}{b_n}x^{m-n}+t_1(x)$ ، نحصل على $f(x)=t(x)g(x)+r(x)$ حيث $r(x), t(x)$ في $F[x]$ و $r(x)=0$ أو $\deg r(x)<\deg g(x)$. بذلك نكون قد برهنا على التمهيدية.

بانتهائنا من البرهنة على التمهيدية أعلاه نكون قد ملأنا الفجوة في تبيان أن $F[x]$ حلقة إقليدية والآن نستطيع أن نقول:

مبرهنة (٣-٩-١)

إن $F[x]$ حلقة إقليدية.

كل النتائج التي حصلنا عليها في بند (٣-٧) تنطبق على الحلقة $F[x]$ وندرجها في التمهيديات أدناه. قد يكون من المفيد أن يحاول القارىء برهنة تلك النتائج مباشرة باستعمال الطرق نفسها المستعملة في البند (٣-٧) في الحلقة الخاصة $F[x]$ وباتخاذ الدرجة كدالة إقليدية.

تمهيدية (٣-٩-٣)

إن $F[x]$ حلقة رئيسة المثالي.

تمهيدية (٣-٩-٤)

إذا كان لدينا كثيرتي حدود $f(x)$ و $g(x)$ في $F[x]$ فإن لهما قاسمًا مشتركا أعْظم $d(x)$ والذي يمكن أن نكتبه على الصيغة $d(x)=\lambda(x)f(x)+\mu(x)g(x)$.

ونسأل الآن: ما الذي يقابل مفهوم العنصر الأولي في $F[x]$ ؟

تعريف

يقال عن كثيرة الحدود $p(x)$ في $F[x]$ إنها غير مختزلة *(irreducible)* على F إذا تحقق *التالي: كلما كان $p(x)=a(x)b(x)$ حيث $a(x)$ و $b(x)$ في $F[x]$ فإن درجة أحد العنصرين $a(x)$ أو $b(x)$ تساوي صفرا (أي أن $a(x)$ أو $b(x)$ يساوي عنصراً في الحقل F) .*

إن خاصة عدم الاختزال تعتمد على الحقل. فعلى سبيل المثال إن كثيرة الحدود x^2+1 غير مختزلة على حقل الأعداد الحقيقية ولكنها تتحلل على الشكل $x^2+1=(x+i)(x-i)$ على حقل الأعداد المركبة (تذكر أن $i^2=-1$) .

تمهيدية (٣-٩-٥)

يمكن كتابة أي كثيرةحدود في $F[x]$ وبصورة وحيدة على شكل حاصل ضرب كثيرات حدود غير مختزلة في $F[x]$.

تمهيدية (٣-٩-٦)

يكون المثالي $A=(p(x))$ في $F[x]$ مثالياً أعظمياً إذا وفقط إذا كانت $p(x)$ غير مختزلة على F .

سنرجع لدراسة الحقل $F[x]/(p(x))$ بتفصيل أكثر في الفصل الخامس من هذا الكتاب لكننا سنحسب الآن مثالاً واحداً.

ليكن F حقل الأعداد النسبية و $p(x)=x^3-2$ عنصراً في $F[x]$. من السهل التحقق من أن $p(x)$ غيرمختزلة على F وبذا يكون $F[x]/(x^3-2)$ حقلاً. نسأل الآن: ما هو شكل عناصر هذا الحقل؟

ليكن $A=(x^3-2)$ أي المثالي في $F[x]$ المتولد بالعنصر x^3-2 . كل عنصر في $F[x]/(x^3-2)$ هو مجموعة مشاركة على الصيغة $f(x)+A$ حيث $f(x)$ في $F[x]$.

بالاستعانة بخوارزم إقليدس نكتب $f(x)=t(x)(x^3-2)+r(x)$ حيث $r(x)=0$ أو $\deg r(x)<\deg(x^3-2)=3$. وهكذا يكون $r(x)=a_0+a_1x+a_2x^2$ حيث a_2,a_1,a_0 في F مما يؤدي إلى أن :

$$f(x)+A=a_0+a_1x+a_2x^2+t(x)(x^3-2)+A=a_0+a_1x+a_2x^2+A$$

لأن $t(x)(x^3-2)$ في A ، وبالتالي يكون

$$f(x)+A=(a_0+A)+a_1(x+A)+a_2(x+A)^2$$

وذلك باستعمال تعريف عمليتي الجمع والضرب في $F[x]/(x^3-2)$. إذا جعلنا $t=x+A$ فإن أي عنصر في $F[x]/(x^3-2)$ هو من الصيغة $a_0+a_1t+a_2t^2$

حيث a_0 ، a_1 ، a_2 في t, F تحقق العلاقة $t^3=2$ في الحقل $F[x]/(x^3-2)$ لأن

$$t^3-2=(x+A)^3-2=x^3-2+A=A=0$$

(تذكر أن A هو العنصر الصفري في الحقل $F[x]/(x^3-2)$) .

كذلك إذا كان $a_0+a_1t+a_2t^2=b_0+b_1t+b_2t^2$

فإن : $(a_0-b_0)+(a_1-b_1)t+(a_2-b_2)t^2=0$

مما يؤدي إلى أن : $(a_0-b_0)+(a_1-b_1)x+(a_2-b_2)x^2$ في A .

ولكن درجة كل كثيرة حدود في A هي 3 على الأقل مما يقودنا إلى أن

$$(a_0-b_0)+(a_1-b_1)x+(a_2-b_2)x^2=0$$

أي أن $a_2=b_2, a_1=b_1, a_0=b_0$.

مما تقدم نستنتج أن أي عنصر في $F[x]/(x^3-2)$ له تمثيل وحيد من الصيغة $a_0+a_1t+a_2t^2$ حيث a_0 ، a_1 و a_2 في F .

بالاستعانة بتمهيدية (٣-٩-٦) نجد أن $F[x]/(x^3-2)$ حقل، بيد أنه من المفيد أن نرى ذلك مباشرة. كل ما نحتاج أن نثبته هو أن لكل عنصر $a_0+a_1t+a_2t^2\neq0$ يوجد معكوس ضربي من الصيغة $\alpha+\beta t+\gamma t^2$. وبناء عليه يجب أن نوجد قيم المجاهيل α ، β و γ في العلاقة

$$(a_0+a_1t+a_2t^2)(\alpha+\beta t+\gamma t^2)=1$$

حيث إن أحد العناصر a_0 ، a_1 ، a_2 لا يساوي صفرا. بضرب القوسين أعلاه واستعمال العلاقة $t^3=2$ نحصل على

$$(a_0\alpha+2a_2\beta+2a_1\gamma)+(a_1\alpha+a_0\beta+2a_2\gamma)t \quad +(a_2\alpha+a_1\beta+a_0\gamma)t^2=1$$

وبذا يكون

$$a_0\alpha+2a_2\beta+2a_1\gamma=1,$$
$$a_1\alpha+a_0\beta+2a_2\gamma=0,$$
$$a_2\alpha+a_1\beta+a_0\gamma=0.$$

دعنا نحاول حل هذه المعادلات ذوات الثلاثة مجاهيل γ,β,α . وعندما نفعل ذلك نجد أنه يوجد حل إذا وفقط إذا كان

$$a_0^3+2a_1^3+4a_2^3-6a_0a_1a_2\neq0$$

لذا فإن مسألة البرهان المباشر على أن $F[x]/(x^3-2)$ حقل تؤول إلى إثبات أن الحل الوحيد في الأعداد النسبية للمعادلة

$$a_0^3+2a_1^3+4a_2^3=6a_0a_1a_2 \qquad (١)$$

هو

$$a_0=a_1=a_2=0$$

نبدأ الآن ببرهنة هذا. لو فرضنا أن هناك حلا في الأعداد النسبية فإنه بالتخلص من المقامات يمكننا أن نثبت أن هناك حلا في الأعداد الصحيحة. لذا يمكننا الفرض أن a_0 ، a_1 ، a_2 أعداد صحيحة تحقق المعادلة (١) كما يمكن الفرض أن الأعداد a_0 ، a_1 ، a_2 ليس لها قاسم مشترك سوى 1 .

لو كان $a_2=b_2d, a_1=b_1d, a_0=b_0d$ حيث d القاسم المشترك الأعظم، بالتعويض في (١) نحصل على

$$d^3(b_0^3+2b_1^3+4b_2^3)=d^3(6b_0b_1b_2)$$

مما يؤدي إلى أن

$$b_0^3+2b_1^3+4b_2^3=6b_0b_1b_2$$

إذن المسألة أصبحت إثبات أن المعادلة (١) ليس لها حل في الأعداد الصحيحة التي تكون أوليه نسبياً. بيد أن (١) تقتضي أن يكون a_0^3 عدداً زوجياً مما يجعل a_0 زوجياً. بالتعويض $a_0=2\alpha_0$ في (١) نحصل على

$$4\alpha_0^3+a_1^3+2a_2^3=6\alpha_0a_1a_2$$

هكـذا نجـد أن α_2^3 وبـالـتـالي α_2 عدد زوجـي، أي $a_1=2\alpha_1$ بالتعـويض في (١) نحصل على

$$2\alpha_0^3+4\alpha_1^3+a_2^3=6\alpha_0\alpha_1a_2$$

إذن العدد 2 قاسم مشترك للأعداد a_0 ، a_1 ، a_2 . هذا يناقض كون هذه الأعداد أولية نسبياً، لذا نكـون قد برهنا على أنه لا يوجد حل في الأعداد النسبية للمعادلة $a_0^3+2a_1^3+4a_2^3=6a_0a_1a_2$ ما عدا الحـل $a_0=a_1=a_2=0$.

إذن يمكننـا أن نجـد قيم المجـاهيل α,β,γ ونكـون قد أثبتنـا بصورة مباشرة أن $F[x]/(x^3-2)$ حقل.

مسائـل

١ - أوجد القاسم المشترك الأعظم لكثيرات الحدود التالية المعرّفة على الأعداد النسبية:

(أ) $x^5-6x+1\ ,\ x^3-6x^2+x+4$

(ب) $x^6+x^3+x+1\ ,\ x^2+1$

٢ - برهن على أن

(أ) x^2+x+1 غير مختزلة على حقل الأعداد الصحيحة قياس 2 .

(ب) x^2+1 غيرمختزلة على الأعداد الصحيحة قياس 7

(جـ) x^3-9 غيرمختزلة على الأعداد الصحيحة قياس 31

(د) x^3-9 غيرمختزلة على الأعداد الصحيحة قياس 11

٣ - ليكن F ، K حقلين و $F \subset K$ وافرض أن f(x) ، g(x) في F[x] وأنهما أوليتان نسبياً في F[x] . برهن على أنهما أوليتان نسبياً في K[x] .

٤ - (ا) برهن على أن x^2+1 غير مختزلة على F ، حقل الأعداد الصحيحة قياس 11 ثم برهن بصورة مباشرة على أن $F[x]/(x^2+1)$ حقل يحوي 121 عنصراً.

(ب) برهن على أن x^2+x+4 غير مختزلة على F ، حقل الأعداد الصحيحة قياس 11 ثم برهن بصورة مباشرة على أن $F[x]/(x^2+x+4)$ حقل يحوي 121 عنصراً.

(جـ)* برهن على أن الحقلين المذكورين في (ا) و (ب) متماثلان.

٥ - ليكن F حقل الأعداد الحقيقية. برهن على أن $F[x]/(x^2+1)$ حقل مماثل لحقل الأعداد المركبة.

*٦ - عرفت **المشتقة** (derivative) (x) لكثيرة الحدود

$$f(x) = a_0+a_1x+\ldots+a_nx^n$$

على أنها

$$f'(x) = a_1+2a_2x+3a_3x^2+\ldots+na_nx^{n-1}$$

برهن على أنه إذا كانت $f(x) \in F[x]$ حيث F حقل الأعداد النسبية فإن f(x) تقبل القسمة على مربع كثيرة الحدود إذا وفقط إذا كانت درجة القاسم المشترك الأعظم d(x) لكثيرتي الحدود f'(x), f(x) أكبر من الصفر.

٧ - إذا كانت $f(x) \in F[x]$ حيث F حقل الأعداد الصحيحة قياس العدد الأولي p وكانت f (x) غير مختزلة على F من الدرجة n . فبرهن على أن $F[x]/(f(x))$ حقل يحوي p^n من العناصر.

(٣-١٠) كثيرات الحدود على حقل الأعداد النسبية

نركِّز دراستنا على كثيرات الحدود التي معاملاتها أعداد نسبية . في أغلب الأحيان ستكون المعاملات أعداداً صحيحة وسندرس خاصة عدم الاختزال لمثل كثيرات الحدود هذه .

تعريف

يقال إن كثيرة الحدود $f(x)=a_0+a_1x+\ldots+a_nx^n$ *حيث* $a_0,a_1,\ldots,a_n$ *أعداد صحيحة ، **بدائي** (primitive) إذا كان القاسم المشترك الأعظم للأعداد* $a_0,a_1,\ldots,a_n$ *يساوي 1 .*

تمهيدية (٣-١٠-١)

إذا كانت $f(x)$, $g(x)$ كثيرتي حدود بدائيتين ، فإن $f(x)\,g(x)$ كثيرة حدود بدائية .

البرهان

لتكن $f(x)=a_0+a_1x+\ldots+a_nx^n$, $g(x)=b_0+b_1x+\ldots+b_mx^m$ وافرض أن التمهيدية غير صحيحة . لذا يوجد عدد صحيح موجب أكبر من 1 يقسم جميع معاملات $f(x)g(x)$ مما يؤدي إلى أن يوجد عدد أولي p يقسم جميع معاملات $f(x)g(x)$.

ولكن $f(x)$ بدائية ، إذن p لا يقسم أحد معاملاتها a_i ليكن a_j أول معامل في $f(x)$ لا يقبل القسمة على p . وبصورة مشابهة دع b_k يكون أول معامل في $g(x)$ لا يقبل القسمة على p . في $f(x)g(x)$ إذا كان c_{j+k} معامل x^{j+k} فإن

$$c_{j+k}=a_jb_k+(a_{j+1}b_{k-1}+a_{j+2}b_{k-2}+\ldots+a_{j+k}b_0)$$
$$+(a_{j-1}b_{k+1}+a_{j-2}b_{k+2}+\ldots+a_0b_{j+k}) \qquad (١)$$

والآن وباختيارنا للمعامل b_k فإن $p|b_{k-1}, p|b_{k-2},\ldots$ ومن ثم

$p|(a_{j+1}b_{k-1}+a_{j+2}b_{k-2}+\ldots+a_{j+k}b_0)$. وبصورة مشابهة $p|a_{j-1}$, $p|a_{j-2}$,...
وبالتالي

$$p|(a_{j-1}b_{k+1}+a_{j-2}b_{k+2}+\ldots+a_0b_{k+j})$$

وبالفرض $p|c_{j+k}$ ، إذن نستنتج من (١) أن $p|a_jb_k$ مما يؤدي إلى أن $p|a_j$ أو $p|b_k$ وكلاهما يناقضان الفرض أعلاه مما يثبت أن التمهيدية يجب أن تكون صحيحة.

تعريف

لتكن $f(x)=a_0+a_1x+\ldots+a_nx^n$ حيث $a_0,a_1\ldots a_n$ أعداد صحيحة. نعرف ***محتوى*** *(content) f(x) على أنه القاسم المشترك الأعظم للأعداد $a_0,a_1,\ldots,a_n$.*

من الواضح أن أي كثيرة حدود $p(x)$ معاملاتها أعداد صحيحة يمكن كتابتها على الهيئة $p(x) = dq(x)$ حيث d محتوى $p(x)$, $q(x)$ كثيرة حدود بدائية.

مبرهنة (٣-١٠-١) (تمهيدية جاوس Gauss'lemma)

إذا كان بالإمكان تحليل كثيرة حدود بدائية إلى حاصل ضرب كثيرتي حدود معاملاتهما أعداد نسبية فإنه من الممكن تحليلها إلى حاصل ضرب كثيرتي حدود معاملاتهما أعداد صحيحة.

البرهان

لنفرض أن $f(x)=u(x)v(x)$ حيث إن معاملات $u(x)$, $v(x)$ أعداد نسبية. بعد التخلص من المقامات واستخراج العوامل المشتركة يمكننا كتابة $f(x)=(a/b)\lambda(x)\mu(x)$ حيث b,a أعداد صحيحة وكل من $\lambda(x)$,$\mu(x)$ كثيرة حدود بدائية.
إذن $bf(x)=a\lambda(x)\mu(x)$.

محتوى الجانب الأيسر هو b لأن $f(x)$ بدائية كما أن $\mu(x)$ و $\lambda(x)$ بدائيتان مما يجعل $\lambda(x)\mu(x)$ بدائية استناداً إلى تمهيدية (٣-١٠-١) وبالتالي يكون محتوى الجانب الأيمن هو a.

إذن $a=b$ أي أن $(a/b)=1$ و $f(x)=\lambda(x)\mu(x)$ حيث إن معـامـلات كل من $\lambda(x),\mu(x)$ أعداد صحيحة . وبهذا ينتهي البرهان .

تعريف

يقال عن كثيرة الحدود أنها ***واحدية بأعداد صحيحة*** *(integer monic)* *إذا كانت جميع معاملاتها أعداداً صحيحة ومعامل حد الدرجة العليا فيها* يساوي 1 .

أي أن كثيرة الحدود الواحدية بأعداد صحيحة تكون على الصيغة $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ حيث $a_1,a_2,\ldots,a_n$ أعداد صحيحة . من الواضح أن كثيرة الحدود الواحدية بأعداد صحيحة هي بدائية .

نتيجة

إذا تحللت كثيرة حدود واحدية بأعداد صحيحة إلى حاصل ضرب كثيرتي حدود غير ثابتتين معاملاتهما أعداد نسبية فإنها تتحلل إلى حاصل ضرب كثيرتي واحديتين بأعداد صحيحة .

نترك برهان هذه النتيجة كتمرين للقارىء .

إن معرفة كون كثيرة الحدود غير مختزلة أصلا ، قد تكون صعبة ومضنية . ولكن توجد بعض المعايير التي تساعدنا على ذلك ، وأحد هذه المعايير هو التالي :

مبرهنة (٣-١٠-٢) (معيار ايزنشتاين)

لتكن $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ كثيرة حدود معاملاتها أعداد صحيحة . إذا وجد عدد أولي p بحيث $p\nmid a_n, p|a_1, p|a_2,\ldots,p|a_0, p^2\nmid a_0$ ، فإن $f(x)$ غير مختزلة على الأعداد النسبية .

البرهان

يمكننا وبدون المساس بعمومية البرهان الفرض أن $f(x)$ بدائية لأن استخراج العامل المشترك الأعظم لمعاملاتها ، لا يؤثر على الفرضية بسبب أن

$p \nmid a_n$. استناداً إلى تمهيدية جاوس إذا تحللت $f(x)$ إلى حاصل ضرب كثيرتي حدود معاملاتهما أعداد نسبية فإنها تتحلل إلى حاصل ضرب كثيرتي حدود معاملاتهما أعداد صحيحة. وهكذا إذا فرضنا أن $f(x)$ مختزلة فإن

$$f(x)=(b_0+b_1x+\ldots+b_rx^r)\ (c_0+c_1x+\ldots+c_sx^s)$$

حيث c_j, b_i أعداد صحيحة و $s>0, r>0$. عند مقارنة المعاملات نجد أن $a_0=b_0c_0$. لكن $p|a_0$ إذن p تقسم b_0 أو c_0 . وحيث إن $p^2 \nmid a_0$ فإنه لا يمكن للعدد p أن يقسم c_0, b_0 معاً. لنفرض أن $p|b_0$ و $p \nmid c_0$ ، لا يمكن للعدد p أن يقسم كل المعاملات $b_0,\ldots,b_r$ لأنه حينئذ p يقسم جميع معاملات $f(x)$ وهذا مخالف للفرض حيث $p \nmid a_n$. ليكن b_k أول معامل بحيث $p \nmid b_k$ ، $k \leq r < n$. أي أن $a_k=b_kc_0+\ b_{k-1}\ c_1+b_{k-2}\ c_2+\ldots+b_0c_k$ بيد أن $p|b_{k-2}, p|b_{k-1}$ . . . الخ. و $p|a_k$ و $p|b_{k-1}$ ، $p|b_{k-2}$ ، . . . ، $p|b_0$ مما يؤدي إلى $p|b_kc_0$. ولكن $p \nmid b_k, p \nmid c_0$ مما يعارض كون $p|b_kc_0$.

وهذا التناقض يبرهن على أن $f(x)$ يجب أن تكون غير مختزلة.

مسائل

١ ـ ليكن F حقل خوارج القسمة لحلقة إقليدية D . برهن تمهيدية جاوس لكثيرات الحدود التي معاملاتها في D والتي تتحلل إلى كثيرات حدود معاملاتها في F .

٢ ـ إذا كان p عدداً أولياً. فبرهن على أن x^n-p غيرمختزلة على الأعداد النسبية.

٣ ـ برهن على أن كثيرة الحدود $1+x+\ldots+x^{p-1}$ ، حيث p عدد أولي، غيرمختزلة على الأعداد النسبية. (إرشاد: اعتبركثيرة الحدود $1+(x+1)+(x+1)^2+\ldots+(x+1)^{p-1}$ ثم استعمل معيار ايزنشتاين).

٤ ـ إذا كان m,n عددين صحيحين أوليين نسبياً وكان $(x-\frac{m}{n})|(a_0+a_1x+\ldots+a_rx^r)$ حيث a_i أعداد صحيحة. برهن على أن $m|a_0$ و $n|a_r$.

٥ ـ إذا كان a عددًا نسبيا و $x-a$ يقسم كثيرة حدود واحدية، بأعداد صحيحة فإن a يجب أن يكون عدداً صحيحاً.

(٣-١١) حلقات كثيرات الحدود على الحلقات الإبدالية

عندما عرفنا حلقة كثيرات الحدود بمتغير واحد على الحقل F لم نستعمل حقيقة كون F حقلاً، كل ما استعملناه أن F حلقة إبدالية. إن حقيقة كون F حقلا وظِّفت فقط لإثبات أن F[x] حلقة إقليدية.

لذا يمكنا تكرار ما عملناه مع الحقول لحلقات أكثر عمومية. عند عملنا ذلك سنفقد بعض الخواص مثل الخاصة الإقليدية ولكن سنرى أن الكثير من الخواص الممتعة تبقى صحيحة. لقد كان بمقدورنا دراسة الموضوع بصورة عامة منذ البداية وكان بإمكاننا الحصول على النتائج الخاصة بالحلقة F[x] بتخصيصنا الحلقة إلى حقل.

لكنا نفضل معالجة الحالات الخاصة قبل أن نبدأ بدراسة الحالات المجردة العامة. إن الثمن الذي ندفعه بهذه الطريقة هو التكرار ولكن هذا يخدم غاية معيّنة وهي توطيد مفاهيمنا السابقة. وبسبب خبرتنا التى اكتسبناها في دراستنا لكثيرات الحدود على الحقول فبإمكاننا أن نترك بعض التفاصيل في البراهين أدناه.

لتكن R حلقة إبدالية بعنصر وحدة. نعرف **حلقة كثيرات الحدود على الحلقة R** ونرمز لها بالرمز R[x] على أنها الرموز الشكلية $a_0+a_1x+\ldots+a_mx^m$ حيث $a_0,a_1,\ldots,a_m$ في R وحيث إن المساواة والجمع والضرب يُعَرَّف بالطريقة نفسها المستعملة في بند (٣ ـ ٩). وكما هي الحال في ذلك البند، R[x] حلقة إبدالية بعنصر وحدة.

الآن نعرف **حلقة كثيرات الحدود في n من المتغيرات على الحلقة R** ونرمز لها بالرمز $R[x_1,\ldots,x_n]$ على النحو التالي: لتكن $R_1=R[x_1]$ ، $R_2=R_1[x_2]$ حلقة كثيرات الحدود في x_2 على R_1 ، . . . . ، $R_n=R_{n-1}[x_n]$ ، نسمي الحلقة R_n حلقة كثيرات الحدود في المتغيرات $x_1,\ldots,x_n$ على R . وعناصر هذه الحلقة هي على الشكل $\sum a_{i_1 i_2\ldots i_n}x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$ حيث إن المساواة وعملية الجمع تتم بمقارنة المعاملات

أما عملية الضرب فتعرف باستخدام قانون التوزيع وقاعدة الأسس

$$(x_1^{i_1}x_2^{i_2}\dots x_n^{i_n})(x_1^{j_1}x_2^{j_2}\dots x_n^{j_n}) = x_1^{i_1+j_1}x_2^{i_2+j_2}\dots x_n^{i_n+j_n}$$

يجب الإشارة إلى أهمية الحالة الخاصة $R=F$ حيث F حقل فنحصل على حلقة كثيرات الحدود في n من المتغيرات على حقل.

مما سيحوز على اهتمامنا هو تأثير بنية الحلقة R على $R[x_1,\dots,x_n]$. وأول نتيجة في هذا الاتجاه هي:

تمهيدية (٣-١١-١)

إذا كانت R حلقة تامة فكذلك تكون $R[x]$.

البرهان

لأجل $0\neq f(x)=a_0+a_1x+\dots+a_mx^m$ حيث $a_m\neq 0$ في $R[x]$ نعرف **درجة** (degree) $f(x)$ على أنها m ، أي أن $\deg f(x)$ هي دليل أعلى معامل غير صفري في $f(x)$. إذا كانت R حلقة تامة فنترك الأمر للقارىء ليبرهن على أن

$$\deg\big(f(x)g(x)\big)=\deg f(x)+\deg g(x).$$

ولكن حينئذ إذا كان $g(x)\neq 0,\ f(x)\neq 0$ فمن المستحيل أن يكون $f(x)g(x)=0$. أي أن $R[x]$ حلقة تامة.

بتكرار استعمال التمهيدية أعلاه نحصل على النتيجة التالية.

نتيجة

إذا كانت R حلقة تامة، فإن $R[x_1,\dots,x_n]$ حلقة تامة.

وبصفة خاصة، إذا كان F حقلاً فإن $F[x_1,\dots,x_n]$ يجب أن تكون حلقة تامة. إذن يمكننا تكوين حقل خوارج القسمة لها وندعوه **حقل الدوال النسبية** (field of rational functions) في $\mathbf{x_1,\dots,x_n}$ على $\mathbf{F}$ ونرمز له بالرمز $F(x_1,\dots,x_n)$. يلعب هذا الحقل دوراً رئيسياً في دراسة الهندسة الجبرية. أما بالنسبة لنا فسيكون ذا أهمية كبرى في دراستنا لنظرية جالوا (Galois Theory) في الفصل الخامس.

في الحقيقـة إننا نريد علاقات أعمق بين بُنْيَتَي $R[x_1,...,x_n]$,R مما تعبّر عنه تمهيدية (٣-١١-١). وفيما سيأتي سنسير بهذا الاتجاه.

كما فعلنا في الحلقات الإقليدية يمكننا التحدث عن قابلية القسمة، الوحدات، الخ في أية حلقـة تامـة R بعـنصر وحـدة. يقـال عن عنصرين b,a في R إنهما **شريكـان** إذا كان a=ub حيث u وحـدة في R. يدعـى الـعنصر a والـذي ليس بوحـدة في R **غير مختزل** irreducible (أو عنصراً أولـياً) وذلـك إذا كان a=bc حيث كل من c,b في R، فإن هذا يقتضي أن يكون b أو c وحدة في R.

إذن العنصر غير المختزل في R هو العنصر الذي لا يمكن تحليله بصورة «غير تافهة».

تعريف

*يقـال عن الحـلقـة التـامـة R بعنصر وحـدة أنها **حلقـة وحيـدة التحليـل** (unique factorization domain) إذا تحقق ما يلي:*

(ا) أي عنصر غير صفري في R إما وحدة أو يمكن كتابته على شكل حاصل ضرب عدد منتهٍ من العناصر غير المختزلة في R.

(ب) إن التحليل في الجزء (ا) وحيد بغض النظر عن الترتيب وشركاء العناصر غير المختزلة.

إن مبرهنـة (٣-٧-٢) تؤكـد أن الحلقـة الإقليدية هي حلقة وحيدة التحليل. أما العكس فهـو غير صحيح. وعـلى سبيل المثـال: الحلقـة $F[x_1,x_2]$ حيث F حقـل ليست رئيسة المثالي (وبالتالي ليست إقليدية) ولكننا سنرى بعد قليل أنها حلقة وحيدة التحليل.

في الصورة العامة للحلقات الإبدالية يمكننا التحدث عن القواسم المشتركة العظمى للعناصر ولكن الصعوبة الأساسية هي أن هذه القواسم قد لا توجد دائماً. لكن في الحلقات الوحيدة التحليل يكون وجود هذه القواسم أمراً مؤكداً. إن برهان هذه الحقيقة ليس صعباً ونتركه كتمرين للقارىء كذلك بقية أجزاء التمهيدية التالية:

تمهيدية (٣-١١-٢)

إذا كانت R حلقة وحيدة التحليل وكان b,a عنصرين في R ، فيوجد في R قاسم مشترك أعظم (a,b) للعنصرين b,a . إضافة إلى ذلك إذا كان b,a أوليين نسبياً (بمعنى $(a,b)=1$) وكان $a|bc$ فإن $a|b$.

نتيجة

إذا كان a في R عنصراً غير مختزل و $a|bc$ فإن $a|b$ أو $a|c$.

الآن نود أن نعمم تمهيدية جاوس (Gauss lemma) (مبرهنة ٣-١٠-١) التي برهناها لكثيرات الحدود التي معاملاتها أعداد صحيحة، إلى الحلقة $R[x]$ ، حيث R حلقة وحيدة التحليل.

نعرف **المحتوى** (content) لكثيرة الحدود $f(x)=a_0+a_1x+...+a_mx^m$ في $R[x]$ على أنه القاسم المشترك الأعظم للمعاملات $a_0,a_1,...,a_m$. إنه وحيد في حدود الوحدات في R . سنرمز لمحتوى $f(x)$ بالرمز $c(f)$. يقال عن كثيرة الحدود في $R[x]$ إنها بدائية إذا كان محتواها يساوي 1 (المقصود وحدة في R). يمكن كتابة أي كثيرة حدود $f(x)$ في $R[x]$ على الصيغة $f(x)=af_1(x)$ حيث $a=c(f)$ و $f_1(x)$ بدائية في $R[x]$ (برهن على ذلك). إن تحليل $f(x)$ إلى حاصل ضرب عنصر في R وكثيرة حدود بدائية في $R[x]$ وحيد بحدود الضرب بوحدة في R .

إن برهان تمهيدية (٣-١٠-١) يسري على الحالة التي نحن بصددها بفارق وحيد، وهو استبدال العدد الأولي p بعنصر غير مختزل في R . لذا يكون لدينا:

تمهيدية (٣-١١-٣)

إذا كانت R حلقة وحيدة التحليل، فإن حاصل ضرب كثيرتي حدود بدائيتين في $R[x]$ هي كثيرة حدود بدائية في $R[x]$.

إذا كانت $g(x), f(x)$ في $R[x]$ فيمكننا أن نكتب $f(x)=af_1(x)$ و $g(x)=bg_1(x)$ ، حيث $a=c(f)$, $b=c(g)$, $g_1(x),f_1(x)$ بدائيتين لذا $f(x)g(x)=abf_1(x)g_1(x)$

استناداً إلى تمهيدية (٣-١١-٣) تكون $f_1(x)g_1(x)$ بدائية، وبالتالي يكون محتوى $f(x)g(x)$ هو ab أي أنه $c(f)c(g)$. بما سبق نكون قد برهنا على النتيجة التالية:

نتيجة

إذا كانت R حلقة وحيدة التحليل و $f(x)$ ، $g(x)$ في $R[x]$ ، فإن $c(fg)=c(f)c(g)$ (إلى حد الوحدات).

بالاستقراء الرياضي البسيط يمكن تعميم النتيجة لتشمل حاصل ضرب عدد منته من كثيرات الحدود فتصبح $c(f_1f_2...f_k)=c(f_1)c(f_2)...c(f_k)$.

لتكن R حلقة تامة وحيدة التحليل، فلكونها حلقة تامة يوجد لها حقل خوارج القسمة F (انظر مبرهنة ٣-٦-١). يمكننا اعتبار $R[x]$ حلقة جزئية من $F[x]$ وإذا كان $f(x)$ عنصراً ما في $F[x]$ فإن $f(x) = f_0(x)/a$ حيث $f_0(x)$ في $R[x]$ و a في R . (أثبت ذلك). من الطبيعي أن نسأل عن العلاقة بين خاصة الاختزال وعدم الاختزال لكثيرة حدود في $R[x]$ باعتبارها عنصراً في الحلقة الأكبر $F[x]$.

تمهيدية (٣-١١-٤)

إذا كانت $f(x)$ في $R[x]$ بدائية وغير مختزلة في $R[x]$، فإنها غير مختزلة في $F[x]$. وبالعكس إذا كانت كثيرة الحدود $f(x)$ بدائية في $R[x]$ وكانت غير مختزلة في $F[x]$ فإنها تبقى غير مختزلة في $R[x]$.

البرهان

لنفرض أن كثيرة الحدود البدائية $f(x)$ فى $R[x]$ غير مختزلة في $R[x]$ ولكنها مختزلة في $F[x]$. لذا $f(x)=g(x)h(x)$ حيث $f(x)$ ، $h(x)$ في $F[x]$ ودرجتاهما موجبتان.

لاحظ أن $h(x)=h_0(x)/b,\ g(x)=g_0(x)/a$ حيث a ، b في R و $g_0(x)$ ، $h_0(x)$ في $R[x]$.

كذلــك $g_0(x)=\alpha g_1(x)$ ، $h_0(x)=\beta h_1(x)$ حيث $\alpha=c(g_0)$ ، $\beta=c(h_0)$ و $g_1(x)$, $h_1(x)$ بدائيتان في $R[x]$. إذن $f(x)=(\alpha\beta/ab)g_1(x)h_1(x)$ مما يؤدي إلى أن $abf(x)=\alpha\beta g_1(x)h_1(x)$. ولكن $g_1(x)h_1(x)$ بدائية استناداً إلى تمهيدية (٣-١١-٣) لذا فإن محتوى الجانب الأيمن يساوي $\alpha\beta$. لما كانت $f(x)$ بدائية، فإن محتوى الجانب الأيسر يساوي ab . وبالتالي نستنتج أن $\alpha\beta=ab$ ومن ثم فإن $f(x)=g_1(x)h_1(x)$ ونكون بذلك قد حصلنا على تحليل غير تافه لكثيرة الحدود $f(x)$ في $R[x]$ وهو مناقض للفرض. لاحظ أن التحليل غير تافه لأن درجة كل من $g_1(x)$ و $h_1(x)$ تساوي درجة $h(x), g(x)$ على الترتيب أي أنهما لا يمكن أن تكونا وحدتين في $R[x]$ (انظر مسألة ٤). نترك الجزء الآخر من التمهيدية كتمرين للقارىء.

تمهيدية (٣-١١-٥)

إذا كانت R حلقة وحيدة التحليل وكانت $p(x)$ كثيرة حدود بدائية في $R[x]$ ، فمن الممكن تحليلها وبصورة وحيدة إلى حاصل ضرب عناصر غير مختزلة في $R[x]$.

البرهان

عند اعتبار $p(x)$ عنصراً في $F[x]$ فإنه، استناداً إلى تمهيدية (٣-٩ - ٥) يمكن تحليله على الصيغة $p(x)=p_1(x)\ldots p_k(x)$ حيث $p_1(x), p_2(x), \ldots, p_k(x)$ عناصر غير مختزلة في $F[x]$. كل من $p_i(x)=f_i(x)/a_i$ حيث $f_i(x)$ في $R[x]$ و a_i في R . وبالإضافة إلى ذلك $f_i(x)=c_i q_i(x)$ حيث $c_i=c(f_i)$ و $q_i(x)$ بدائيــة في $R[x]$. لذا $p_i(x)=c_i q_i(x)/a_i$، حيث c_i, a_i في R و $q_i(x)$ بدائية في $R[x]$. لما كانت $p_i(x)$ غير مختزلة في $R[x]$ فإن $q_i(x)$ يجب أن تكون غير مختزلة في $R[x]$ وباستعمال تمهيدية (٣-١١-٤) نستنتج أن $q_i(x)$ غير مختزلة في $R[x]$.

الآن

$$p(x)=p_1(x)\ldots p_k(x)=\frac{c_1c_2\ldots c_k}{a_1a_2\ldots a_k}q_1(x)\ldots q_k(x)$$

مما يؤدي إلى أن $a_1a_2\ldots a_k p(x)=c_1c_2\ldots c_k q_1(x)\ldots q_k(x)$. بيد أن $p(x)$ بدائية، وكذلك $q_1(x)$ ، . . . ، $q_k(x)$ إذن محتــوى الجــانــب الأيسر هو $a_1a_2\ldots a_k$ والجــانــب الأيمن هو

$c_1c_2...c_k$ مما يجعـل $c_1c_2...c_k$ = $a_1a_2...a_k$ ومن ثم $p(x)=q_1(x)...q_k(x)$. بذا نكون قد حللنا $p(x)$ في $R[x]$ إلى حاصل ضرب عناصر غير مختزلة .

ونسأل الآن : هل من الممكن تحليل $p(x)$ بطريقة أخرى؟ .إذا كانت $p(x)=r_1(x)...r_l(x)$ حيث $r_i(x)$ غير مختزلة في $R[x]$. ولما كانت $p(x)$ بدائية فإنه يجب أن تكون كل من $r_i(x)$ بدائية وبالتالي **غير مختزلة في** $F[x]$ وفقاً لتمهيدية **(٣-١١-٤)** . ولكن $F[x]$ حلقة وحيدة التحليل حسب تمهيدية (٣-٩-٥) فنستنتج أن $k=l$ ، وبعد إعادة الترتيب $r_i(x)=q_i(x)$ (بغض النظر عن الشركاء) وبناءاً عليه يكون للعنصر $p(x)$ تحليل وحيد إلى حاصل ضرب عناصر غير مختزلة في $R[x]$.

الآن نكون قد جمعنا المعلومات الضرورية لإثبات المبرهنة الرئيسة في هذا البند.

مبرهنة (٣-١١-١)

إذا كانت R حلقة وحيدة التحليل فكذلك تكون R[x] .

البرهان

ليكن $f(x)$ عنصراً اختيارياً في $R[x]$. يمكننا كتابة $f(x)$ بطريقة وحيدة على الشكل $f(x)=cf_1(x)$ حيث $c=c(f)$ في R و $f_1(x)$ بدائية في $R[x]$. وفقاً لتمهيدية **(٣-١١-٥)** يمكن تحليل $f_1(x)$ بصورة وحيدة إلى حاصل ضرب عناصر غير مختزلة في $R[x]$. وماذا عن العنصر c ؟ لو فرضنا أن $c=a_1(x)a_2(x)...a_m(x)$ في $R[x]$ ، فإن

$$0=\deg c=\deg(a_1(x))+\deg(a_2(x))+\ldots+\deg(a_m(x)) .$$

إذن يجب أن تكون درجة أي من $a_i(x)$ صفراً، أي أنه عنصر في R . وبعبارة أخرى يكون التحليل الوحيد للعنصر c كعنصر في $R[x]$ هو على شكل حاصل ضرب عناصر في R . وعلى وجه الخصوص يبقى العنصر غير المختزل في R عنصراً غير مختزل في $R[x]$. ولما كانت R حلقة وحيدة التحليل، فإن c تتحلل بصورة وحيدة إلى حاصل ضرب عناصر غير مختزلة في R وبالتالي في $R[x]$.

عند وضعنا في نظر الاعتبار التحليل الوحيد للعنصر $f(x)$ إلى $cf_1(x)$ حيث $f_1(x)$ بدائية و c في R والتحليل الوحيد للعنصر c والعنصر $f_1(x)$ نكون قد أثبتنا ما نريده في هذه المبرهنة.

إذا كانت R حلقة وحيدة التحليل، فإن $R_1=R[x_1]$ حلقة وحيدة التحليل كذلك. لذا $R_2=R_1[x_2]=R[x_1,x_2]$ تكون حلقة وحيدة التحليل. وبالاستمرار على هذا النمط نحصل على:

نتيجة (١)

إذا كانت R حلقة وحيدة التحليل فكذلك $R[x_1,...,x_n]$.

هناك حالة خاصة من نتيجة ١ مهمة بحد ذاتها وهي:

نتيجة (٢)

إذا كان F حقلاً فإن $F[x_1,...,x_n]$ حلقة وحيدة التحليل.

مسائل

١ - برهن على أن $R[x]$ حلقة إبدالية بعنصر وحدة إذا كانت R كذلك.

٢ - برهن على أن $R[x_1,...,x_n] = R[x_{i_1},...,x_{i_n}]$ حيث $(i_1,...,i_n)$ تبديل من $(1,2,...,n)$.

٣ - إذا كانت R حلقة تامة فبرهن على أن

$$\deg(f(x)g(x)) = \deg(f(x))+\deg(g(x))$$

حيث $f(x)$ ، $g(x)$ في $R[x]$.

٤ - إذا كانت R حلقة تامة بعنصر وحدة فبرهن على أن أية وحدة في $R[x]$ هي وحدة في R .

٥ - لتكن R حلقة إبدالية لا تحوي عناصر معدومة القوة غير صفرية (أي $a^n=0$ تقتضي $a=0$). إذا كانت $f(x)=a_0+a_1x+...+a_mx^m$ في $R[x]$ قاسماً للصفر. فبرهن على أنه يوجد عنصر $b\neq 0$ في R بحيث $ba_0=ba_1=...=ba_m=0$.

٦*- حل المسألة ٥ بحذف فرضية أن R لا تحوي عناصر معدومة القوة غير صفرية.

٧*- إذا كانت R حلقة إبدالية بعنصر وحدة فبرهن على أن $a_0+a_1x+...+a_nx^n$ في $R[x]$ له معكوس ضربي في $R[x]$ (بمعنى أنه وحدة في $R[x]$) إذا وفقط إذا كان a_0 وحدة في R وكانت $a_1,...,a_n$ عناصر معدومة القوة.

٨ - برهن على أنه إذا كان F حقلاً فإن $F[x_1,x_2]$ ليست حلقة رئيسة المثالي.

٩ - برهن بالتفصيل تمهيدية ٣-١١-٢ ونتيجتها.

١٠ - (ا) إذا كانت R حلقة وحيدة التحليل فبرهن على أنه يمكن كتابة أي عنصر $f(x)$ في $R[x]$ على الشكل $f(x)=af_1(x)$ حيث a في R و $f_1(x)$ بدائية.

(ب) برهن على أن التحليل في الجزء (ا) وحيد (بغض النظر عن الشركاء).

١١ - إذا كانت R حلقة تامة وكان F حقل خوارج القسمة لها. فبرهن على أنه يمكن كتابة أي عنصر $f(x)$ في $F[x]$ على الصيغة $f(x)=f_0(x)/a$ حيث $f_0(x)$ في $R[x]$ و a في R.

١٢ - برهن على الجزء العكسي في تمهيدية (٣-١١-٤).

١٣ - برهن على النتيجة الثانية لمبرهنة (٣-١١-١).

١٤ - برهن على أن أية حلقة رئيسة المثالي هي حلقة وحيدة التحليل.

١٥ - إذا كانت Z حلقة الأعداد الصحيحة فبرهن على أن $Z[x_1,\dots,x_n]$ حلقة وحيدة التحليل.

مسائل إضافية

١ - لتكن R حلقة إبدالية. يقال عن مثالي P من R إنه **مثالي أولي** إذا كان لأي عنصرين b,a في R بحيث $ab\in P$ يقتضي أن $a\in P$ أو $b\in P$. برهن على أن P مثالي أولي في R إذا وفقط إذا كانت R/P حلقة تامة.

٢ - لتكن R حلقة إبدالية بعنصر وحدة. برهن على أن كل مثالي أعظمي في R هو مثالي أولي.

٣ - أعط مثالا على حلقة تحوي مثالياً أولياً ولكنه ليس أعظمياً.

٤ - إذا كانت R حلقة إبدالية منتهية (بمعنى أنها تحوي عدداً مُنْتهياً من العناصر) بعنصر وحدة، فبرهن على أن كل مثالي أولي في R هو مثالي أعظمي.

٥ - إذا كان F حقلا فبرهن على أن $F[x]$ يماثل $F[t]$.

٦ - أوجد جميع التماثلات الذاتية σ للحلقة $F[x]$ والتي تحقق العلاقة $\sigma(f)=f$ لكل عنصر f في F.

٧ - إذا كانت R حلقـة إبـدالية و N مجموعة كل العناصر x في R بحيث أن $x^n=0$ حيث n عدد صحيح اختياري . برهن على ما يلي:

(ا) N مثالي في R

(ب) في $\bar{R}=R/N$ إذا كان $(\bar{x})^m=0$ لعدد ما m فإن $\bar{x}=0$.

٨ - لتكن R حلقـةً إبـداليةً و A مثـالياً في R . إذا كانت N(A) مجموعة العناصر x في R بحيث $x^n \in A$ حيث n عدد صحيح اختياري . فبرهن على أن

(ا) N(A) مثالي في R يحتوي A

(ب) $N(N(A))=N(A)$

يدعى N(A) **جذر** (radical) المثالي A .

٩ - لتكن Z_n حلقة الأعداد الصحيحة قياس n . صف المثالي N (المذكور في مسألة ٧) في الحلقة Z_n بدلالة n .

١٠ - إذا كان A و B مثـاليين في حلقـة R بحيث $A\cap B=(0)$. فبرهن على أنـه لكـل a في A و b في B يجب أن يكون $ab=0$.

١١ - لتكن R حلقـة و Z(R) مجمـوعـة كل العنـاصر x في R بحيث $xy=yx$ لجميع العناصر y في R . برهن على أن Z(R) حلقة جزئية من R .

١٢ - إذا كانت R حلقة قسمة فبرهن على أن Z(R) حقلاً .

١٣ - أوجد كثيرة حدود من الدرجة الثالثة غير مختزلة على حلقة الأعداد الصحيحة قياس 3 ، ثم استعملها لبناء حقل يحوي سبعة وعشرين عنصراً .

١٤ - كون حقلاً يحوي ٦٢٥ عنصراً .

١٥ - *إذا كان F حقلاً و* $p(x) \in F[x]$. *فبرهن على أنه في الحلقة* $R=\dfrac{F[x]}{(p(x))}$

يكـون المثـالي N (انـظر مسـألـة ٧) مسـاوياً للمثـالي (0) إذا وفقط إذا كانت $p(x)$ لا تقبل القسمة على مربع كثيرة حدود .

١٦ - برهن على أن كثيرة الحدود $f(x)=1+x+x^3+x^4$ مختزلة على أي حقل

١٧ - برهن على أن كثيرة الحدود $f(x)=x^4+2x+2$ غير مختزلة على حقل الأعداد النسبية .

١٨ ـ إذا كان F حقلاً منتهيا فبرهن على أن مميزه يجب أن يكون عدداً أوليًا p وأن F يحوي على p^n من العناصر فقط، حيث n عدد صحيح. أثبت أيضا أن $a^{p^n}=a$ لكل a في F.

١٩ ـ برهن على أن أي مثالي غير صفري في حلقة أعداد جاوس الصحيحة $Z[i]$ يجب أن يحوي عدداً صحيحاً موجباً.

٢٠ ـ إذا كانت R حلقة فيها $a^4=a$ لكل a في R. فبرهن على أن R يجب أن تكون إبدالية.

٢١ ـ إذا كانت R و R' حلقتين و ϕ تطبيق من R إلى R' يحقق:

(ا) $\phi(x+y)=\phi(x)+\phi(y)$ لكل y,x في R.

(ب) $\phi(xy)=\phi(x)\phi(y)$ أو $\phi(y)\phi(x)$، فبرهن على أنه لكل b,a في R $\phi(ab)=\phi(a)\phi(b)$ أو أنه لكل b,a في R $\phi(ab)=\phi(b)\phi(a)$.

(تلميح: لكل a في R دع $W_a=\{x\in R|\phi(ax)=\phi(a)\phi(x)\}$ و $V_a=\{x\in R|\phi(ax)=\phi(x)\phi(a)\}$).

٢٢ ـ إذا كانت R حلقة بعنصر الوحدة 1 وفيها $(ab)^2=a^2b^2$ لجميع b,a في R. فبرهن على أن R حلقة إبدالية.

٢٣ ـ أورد مثالاً على حلقة غير إبدالية (طبعاً بدون عنصر وحدة 1) والتي فيها $(ab)^2=a^2b^2$ لجميع العناصر b,a في R.

٢٤ ـ (ا) لتكن R حلقة بعنصر الوحدة 1 بحيث $(ab)^2=(ba)^2$ لجميع العناصر b,a في R. برهن على أن R إبدالية إذا كانت $2x=0$ تقتضي $x=0$ لكل x في R.

(ب) بين أن النتيجة في (ا) تكون خاطئة إذا كانت $2x=0$ لعنصر ما $x\neq0$ في R.

(جـ) إذا كان $2x=0$ يقتضي أن $x=0$ في R فبين أن النتيجة في (ا) تكون خطأ إذا كانت R لا تحوي عنصر وحدة.

٢٥ ـ إذا كانت R حلقة فيها $x^n=0$ تقتضي أن $x=0$ وإذا كان $(ab)^2=a^2b^2$ لجميع العناصر b,a في R. فبرهن على أن R يجب أن تكون إبدالية.

٢٦ ـ إذا كانت R حلقة فيها $x^n=0$ تقتضي أن $x=0$. إذا كان $(ab)^2=(ba)^2$ لجميع العناصر b,a في R . فبرهن على أن R يجب أن تكون إبدالية.

٢٧ ـ إذا كانت p_1 ، p_2 ، . . . ، p_k أعداداً أولية مختلفة وكانت $n=p_1p_2\cdots p_k$. فبرهن على أنه في الحلقة Z_n يوجد بالتحديد 2^k من العناصر a التي تحقق العلاقة $a^2=a$.

٢٨ ـ كوِّن كثيرة حدود $q(x)\neq 0$ معاملاتها أعداد صحيحة بحيث يمكننا حل التطابق $q(x)\equiv 0$ قياس p لأي عدد أولي p بينما لا يوجد حل للمعادلة $q(x)=0$ في الأعداد النسبية.

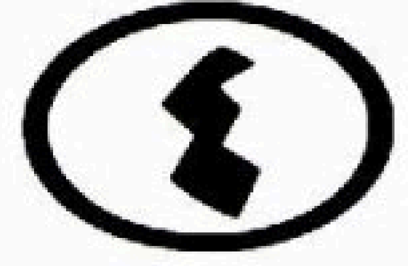
لقراءتك الإضافية هذه بعض المصادر

Zariski, Oskar, and Samuel, Pierre. *Commutative Algebra*, Vol. 1. Princeton, New Jersey: D. Van Nostrand Company, Inc., 1958.

Mc Coy, N.H. *Rings and Ideals*. Carus Monograph No.8. La Salle, Illinois: Open Court Publishing Company, 1948.

مواضيع للمناقشة الصفيّة

Motzkin, T. "The Euclidean algorithm." *Bulletin of the American Mathematical Society,* Vol.55 (1949), 1142–1146.



فضاءات المتجهات والفضاءات الحلقية

● مفاهيم أساسية ● الاستقلال الخطي والأساسات
● الفضاءات الثنوية ● فضاءات الضرب الداخلي
● الفضاءات الحلقية .

في الفصلين الماضيين ، قدّمنا الزمر والحلقات وقد دفعنا إلى دراسة الزمر مجموعة التطبيقات الأحادية لمجموعة على نفسها أما الحلقات فتكمن جذورها في مجموعة الأعداد الصحيحة . إن النموذج الجبري الثالث الذي سنُعنى بدراسته ـ وهو **فضاء المتجهات** (vector space) ـ يرجع أصله في الغالب إلى مواضيع في الفيزياء والهندسة .

إن وصف فضاء المتجهات سيذكرنا بالزمر والحلقات ـ بل إن جزءا من بنيته هو زمرة إبدالية ـ ولكن فضاء المتجهات يختلف عن سابقيه من البنى الجبرية في أن إحدى العمليات المعرّفة عليه تستعمل عناصر خارج المجموعة نفسها . سوف تتضح هذه الملاحظات حين نقدّم تعريف فضاء المتجهات .

إن أهمية فضاءات المتجهات تعود إلى حقيقة أن الكثير من النماذج التي تظهر في حلول مسائل معيّنة تبدو على شكل فضاءات متجهات . لهذا السبب فإن المفاهيم الأساسية التي تتضمنها هذه الفضاءات لها خاصة الشمولية ، وسوف نواجهها في مواضع مختلفة . من بين هذه الأفكار الأساسية هي الارتباط الخطي والأساس والبعد والتي سوف ندرسها في هذا الفصل . إن هذه الأفكار تعتبر وسائل قوية وفعّالة في جميع فروع الرياضيات وسوف نستعين بها في العديد من المواقع الرئيسة من الفصل الخامس الذي يُعنى بدراسة نظرية الحقول .

إن الفصل السادس من هذا الكتاب سيخصص لدراسة التشاكلات من فضاء متجهات إلى آخر (أو إلى نفسه)، والتي لا يمكن الاستغناء عنها في دراسة متكاملة لفضاءات المتجهات.

في الجزء الأخير من هذا الفصل سوف نعمم فكرة فضاءات المتجهات إلى الفضاءات الحلقية. وعموماً تعتبر الفضاءات الحلقية فضاءات متجهات على حلقة بدلاً من حقل. سوف نثبت المبرهنة الأساسية للفضاءات الحلقية المنتهية التوليد على الحلقات الإقليديه. هذه المبرهنة سوف تعطينا وصفاً كاملاً لِبِنْيَة الزمر الإبدالية المولّدة بعدد منتهٍ من العناصر.

(٤-١) مفاهيم أساسية

تعريف

*يقال عن مجموعة غير خالية V إنها **فضاء متجهات** (vector space) على حقل F إذا كانت V زمرة إبدالية بالنسبة إلى عملية نرمز لها بالرمز + وإذا كان لأي عنصر α في F و v في V يوجد عنصر في V نكتبه على الصيغة αv ويحقق ما يلي:*

(١) $\alpha(v+w)=\alpha v+\alpha w$

(٢) $(\alpha+\beta)v=\alpha v+\beta v$

(٣) $\alpha(\beta v)=(\alpha\beta)v$

(٤) $1v=v$

لكل العناصر β,α في F و w,v في V (حيث 1 تمثل عنصر الوحدة في F بالنسبة إلى عملية الضرب).

لاحظ في المسلّمة (١) أعلاه العملية + هي تلك المعرفة على V بينما في الجانب الأيسر من المسلّمة (٢)، العملية + هي المعرفة على الحقل F والجانب الأيمن هي عملية V .

فيما سيأتي ستعتمد الرموز التالية:

ا) الحرف F يرمز للحقل.

ب) الحروف اليونانية الصغيرة ترمز لعناصر الحقل F والتي سندعوها **قياسيات**.
جـ) الحروف اللاتينية الكبيرة ترمز لفضاءات متجهة على F .
د) الحروف اللاتينية الصغيرة ترمز لعناصر فضاءات المتجهات والتي سوف ندعوها **متجهات** (vectors) .

إذا نظرنا إلى V على أنه زمرة إبدالية بالنسبة للعملية + وأهملنا العملية الأخرى فالمسلمة (١) تنص على أن ضرب عناصر V بقياسي معين α يعرف تشاكلا من الزمرة الإبدالية V إلى نفسها. سنبين في تمهيدية (٤-١-١) أنه إذا كان $\alpha\neq0$ فإن هذا التشاكل هو تماثل من V على V .

هذا يدل على أن وُجوهاً كثيرة من نظرية فضاءات المتجهات (ومن الحلقات أيضا) يمكن تطويرها كجزء من نظرية الزمر لو أننا عممنا فكرة الزمرة إلى **الزمرة مع مؤثرات** (group with operators) . وبالنسبة للطلبة الذين اعتادوا على شيء من الجبر المجرد، هذه هي وجهة النظر المفضّلة ولكننا افترضنا أن القارىء لم يألف الجبر المجرد مما جعلنا نشعر أن هذه الوسيلة قد تقودنا إلى دخول مفاجيء إلى أفكار المادة دون أن تكون خبرتنا هي مرشدنا إلى ذلك.

مثال (٤-١-١)

ليكن K,F حقلين بحيث إن F حقل جزئي من K . يمكننا اعتبار K فضاء متجهات على F باتخاذنا عملية الجمع في K كعملية + لهذا الفضاء وبتعريف αv لعنصر α في F و v في K على أنه حاصل الضرب αv كعناصر من الحقل K . عندئذ تتحقق المسلمات ١، ٢، ٣ لفضاء المتجهات كنتيجة من قانون التوزيع الأيمن وقانون التوزيع الأيسر وقانون التجميع على الترتيب والتي تتحقق باعتبار K حلقة.

مثال (٤-١-٢)

ليكن F حقلا و V جميع العديدات من رتبة n $(\alpha_1,\ldots,\alpha_n)$ حيث α_i في F .

يكـون الـعـنصران $(\alpha_1,\dots,\alpha_n)$ و $(\beta_1,\dots,\beta_n)$ متـسـاويين إذا وفـقط إذا كان $\alpha_i=\beta_i$ لكل $i=1,2,\dots,n$.

الآن نعـرف العمليات الـلازمة على V لنجعـل منه فضاء متجهات على F كالتالي:

(١) $(\alpha_1,\dots,\alpha_n)+(\beta_1,\dots,\beta_n) = (\alpha_1+\beta_1,\alpha_2+\beta_2,\dots,\alpha_n+\beta_n)$

(٢) $\gamma(\alpha_1,\dots,\alpha_n)=(\gamma\alpha_1,\dots,\gamma\alpha_n)$ لجميع γ في F .

من السهـل أن نتحقق من أن V بالعمليتـين أعـلاه هو فضاء متجهات على F ونرمز له بالرمز $F^{(n)}$.

مثال (٤-١-٣)

ليكن F حقـلا ما وV هي F[x] مجمـوعـة كثـيرات الحـدود في x على F . مع عمـلية الجـمـع لكثـيرات الحـدود وعـملية ضرب كثـير حدود بعنصر من F يكون F[x] فضاء متجهات على F .

مثال (٤-١-٤)

في F[x] لتكن V_n مجموعة كثيرات الحدود التي درجتها أقـل من n . باستعمال عملية الجمـع المعتـادة لكثـيرات الحـدود وكـذلـك الضرب بعنصر من F يكـون V_n فضاء متجهات على F .

ونسأل الآن: ما هي العلاقة بين المثال (٤-١-٤) والمثال (٤-١-٢)؟ كل عنصر من V_n هو على الشكل $\alpha_0+\alpha_1x+\dots+\alpha_{n-1}x^{n-1}$ حيث $\alpha_i\in F$. إذا طبقنا هذا العنصر على $(\alpha_0,\alpha_1,\dots,\alpha_{n-1})$ في $F^{(n)}$ يمكننا توقع تماثل V_n مع $F^{(n)}$ وذلك بعد أن نعرّف التشاكل والتماثل بين فضاءات المتجهات.

تعريف

إذا كانـت W مجمـوعـة جزئية من فضـاء المتجهـات V على F فيقـال إن W

فضاء جزئي *(subspace) من V إذا كونت W فضاء متجهات على F بالنسبة للعمليات المعرّفة على V .*

وبعبارة مكافئة يقال إن W فضاء جزئي من V إذا كان $\alpha w_1+\beta w_2 \in W$ لأي عنصرين w_1, w_2 في W و β,α في F .

لاحظ أن فضاء المتجهات المعرف في مثال (٤-١-٤) هو فضاء جزئي من الذي عُرّف في مثال (٤-١-٣). يمكن للقارىء أن يجد أمثلة أخرى على فضاءات المتجهات والفضاءات الجزئية في المسائل التي تلي هذا البند.

تعريف

إذا كان V, U فضائي متجهات على F فيقال عن التطبيق T من U إلى V إنه ***تشاكل*** *(homomorphism) إذا كان*

$$(u_1+u_2)T=u_1T+u_2T \quad (1)$$

$$(\alpha u_1)T=\alpha(u_1T) \quad (2)$$

لجميع العناصر u_2,u_1 في U و α في F .

كما حصل في نماذجنا السابقة فإن التشاكل هو تطبيق يحفظ البنية الجبرية للنظام. إذا كان التشاكل T تطبيقا أحاديا فيسمى **تماثلا**. تعرف نواة T على أنها المجموعة $\{u \in U | uT=0\}$ حيث 0 هو العنصر المحايد لعملية الجمع في V . إن نواة T هي فضاء جزئي من U ويكون T تماثلا إذا وفقط إذا كانت نواته تساوي (0) (نترك البرهان كتمرين للقارىء). يقال عن فضائي متجهات إنهما **متماثلان** إذا وجد تماثل من أحدهما على الآخر.

سنرمز لمجموعة التشاكلات من U إلى V بالرمز $\mathrm{Hom}(U,V)$ وسنهتم بصورة خاصة بالمجموعتين $\mathrm{Hom}(U,U), \mathrm{Hom}(U,F)$. سنقوم بدراسة أولى المجموعتين أدناه أما الثانية والتي يمكن البرهان على أنها حلقة فتسمى **حلقة التحويلات**

على U (ring of linear transformations) . سنخصص جزءا كبيرا من هذا الكتاب لدراسة Hom (U,U) بصورة مفصّلة .

الآن نبدأ دراستنا بتمهيدية حول العمليات في فضاءات المتجهات والتي تسهل علينا إجراء بعض الحسابات البسيطة . في منطوق التمهيدية 0 يمثل صفر عملية الجمع في V و o يمثل الصفر في v, F− المعكوس الجمعي للعنصر v في V .

تمهيدية (٤-١-١)

إذا كان V فضاء متجهات على F فإن

(١) $\alpha 0=0$ لكل α في F .

(٢) $ov=0$ لكل v في V

(٣) $(-\alpha)v=-(\alpha v)$ لكل α في F و v في V .

(٤) إذا كان $v\neq 0$ فإن $\alpha v=0$ تقتضي أن $\alpha=0$.

البرهان

إن البرهان سهل جداً ويتبع الخطوات نفسها التي اتبعناها لبرهنة نتائج مماثلة في الحلقات .

لذا فسنتجنب التفاصيل ونقدم البرهان مختصرا :

(١) لما كان

$$\alpha 0=\alpha(0+0)=\alpha 0+\alpha 0$$

فإننا نجد أن

$$\alpha 0=0$$

(٢) لما كان

$$ov=(o+o)v=ov+ov$$

فإننا نجد أن

$$ov=0$$

(٣) لما كان

$$0=(\alpha+(-\alpha))v=\alpha v+(-\alpha)v$$

فإننا نجد

$$(-\alpha)v=-(\alpha v)$$

(٤) إذا كان $\alpha\neq 0, \alpha v=0$ ، فإن

$$0=\alpha^{-1}0=\alpha^{-1}(\alpha v)=(\alpha^{-1}\alpha)v=1v=v$$

إن التمهيدية التي انتهينا من برهانها تبين أن الضرب بالعنصر الصفري في V أو بالعنصر الصفري في F ينتج عنه العنصر الصفري في V . لذا فإننا سنستعمل الرمز نفسه لكلا العنصرين الصفريَّيْن دون أن يسبب ذلك لبساً للقارىء.

إذا كان V فضاء متجهات على W,F فضاءاً جزئياً من V فباعتبارهما مجرد زمرتين إبداليتين ننشيء الزمرة الخارجة V/W التي عناصرها المجموعات المشاركة v+W حيث v في V . إن إبدالية عملية الجمع وما بيناه في الفصل الثاني في نظرية الزمر يجعلان V/W زمرة إبدالية. . الآن نجعل من V/W فضاء متجهات ومن أجل ذلك نعرف $\alpha(v+W)$ على أنه $\alpha v+W$ حيث $v+W\in V/W$ و $\alpha\in F$. كما هو معتاد يجب أن نثبت أن العملية أعلاه حسنة التعريف. أي إذا كان $v+W=v'+W$ فإن $\alpha(v+W)=\alpha(v'+W)$. ومن أجل ذلك لاحظ أن $v-v'$ في W لأن $v+W=v'+W$. ولكن W فضاء جزئي مما يجعل $\alpha(v-v')$ في W . باستعمال الجزء ٣ من تمهيدية (٤-١-١) (انظر مسألة ١) نجد أن $\alpha v-\alpha v'\in W$ أي أن $\alpha v+W=\alpha v'+W$. وهكذا $\alpha(v+W)=\alpha v+W=\alpha v'+W=\alpha(v'+W)$ مما يثبت أن هذه العملية حسنة التعريف.

إن التحقق من استيفاء V/W لجميع شروط فضاء المتجهات أمر رتيب نتركه للقارىء. بما سبق نكون قد برهنا على التمهيدية الآتية:

تمهيدية (٤-١-٢)

إذا كان V فضاء متجهات على F و W فضاء جزئيا من V ، فإن V/W فضاء متجهات على F بحيث إنه لأي عنصرين v_2+W, v_1+W في V/W ولأي α في F يكون

$$(v_1+W)+(v_2+W)=(v_1+v_2)+W \qquad (1)$$

$$\alpha(v_1+W)=\alpha v_1+W \qquad (2)$$

*يطلق على V/W **الفضاء الخارج** quotient space من V على W .*

الآن نذكر مبرهنة التشاكل الأولى لفضاءات المتجهات بدون برهان ولكننا ندعو القارىء للعودة إلى برهان مبرهنة (٢-٧-١).

مبرهنة (٤-١-١)

إذا كان T تشاكلا من U على V نواته W ، فإن V يماثل U/W . وبالعكس إذا كان U فضاء متجهات و W فضاءً جزئياً من U فيوجد تشاكل من U على U/W .

يجد القارىء مبرهنات التشاكل الأخرى في المسائل التي تلي هذا البند.

تعريف

*ليكن V فضاء متجهات على F و $U_1,\dots,U_n$ فضاءات جزئية في V . يقال عن V إنه **الجمع المباشر الداخلي** (internal direct sum) للفضاءات $U_1,\dots,U_n$ إذا أمكن كتابة كل عنصر v في V بطريقة وحيدة فقط على الصيغة $v=u_1+u_2+\dots+u_n$ حيث $u_i \in U_i$.*

لتكن $V_1,\dots,V_n$ فضاءات متجهات على F، V مجموعة العديدات $(v_1,\dots,v_n)$ من رتبة n ، حيث v_i في V_i . يكون العنصران $(v_1,\dots,v_n)$ و $(v'_1,\dots,v'_n)$ من V متساويين إذا وفقط إذا كان $v_i=v'_i$ لكل i . نعرّف حاصل الجمع لعنصرين من V بالطريقة التالية :

$$(v_1,\dots,v_n)+(w_1,\dots,w_n)=(v_1+w_1,v_2+w_2,\dots,v_n+w_n)$$

وأخـيراً إذا كان α في F و $(v_1,...,v_n)$ في V نعـرّف $\alpha(v_1,...,v_n)$ على أنـه $(\alpha v_1,\alpha v_2,...,\alpha v_n)$.

من السهل التحقق من أن العمليات المعرّفة على V أعلاه تجعل منه فضاء متجهات على F . ندعو V الجمع المباشر الخارجي للفضاءات $V_1,...,V_n$ ونرمز لذلك بكتابة

$$V=V_1\oplus...\oplus V_n$$

مبرهنة (٤-١-٢)

إذا كان V يساوي الجمع المباشر الداخلي للفضاءات الجزئية $U_1,...,U_n$ ، فإن V يماثل الجمع المباشر الخارجي لفضاءات المتجهات $U_1,...,U_n$.

البرهان

إذا كان v في V فإنـه من الفـرض يمكن كتـابتـه بصـورة وحيدة على الشكـل $v=u_1+u_2+...+u_n$ حيث u_i في U_i ، نعـرف التـطبيق T من V إلى $U_1\oplus...\oplus U_n$ على النحو $vT=(u_1,...,u_n)$. التطبيق T حسن التعريف لأن v له تمثيل وحيد على الصيغة أعـلاه ومـن الـواضـح أن T غامـر ذلـك لأن أي عنصر اخـتـياري $(w_1,...,w_n)$ في $U_1\oplus...\oplus U_n$ يسـاوي wT حيث $w=w_1+...+w_n$ في V . نترك للقـارىء برهـان أن T أحادي وأنه تشاكل .

بسبب التماثل المذكور في مبرهنة (٤-١-٢) فإننا فيما سيأتي سوف نتحدث عن الجمع المباشر دون أن نذكر كونه خارجياً أم داخلياً .

مسائل

١ - بين أنه في فضاء المتجهات يكون $\alpha(v-w)=\alpha v-\alpha w$.

٢ - برهن على أن فضائي المتجهات المذكورين في المثال ٤-١-٤ والمثال ٤-١-٢ متماثلان .

٣ - برهن على أن نواة التشاكل تكوِّن فضاء جزئياً .

٤ - (ا) إذا كان F حقل الأعداد الحقيقية فبين أن مجموعة الدوال المتصلة حقيقية القيم المعرفة على الفترة المغلقة $[0,1]$ تكوِّن فضاء متجهات على F .

(ب) برهن على أن الدوال التي توجد مشتقاتها من رتبة n من الدوال المذكورة في الجزء (ا) تكوِّن فضاء جزئياً لقيم $n=1,2,\ldots$.

٥ - (ا) ليكن F حقل الأعداد الحقيقية و V مجموعة المتتابعات $(a_1,a_2,\ldots,a_n,\ldots)$ حيث a_i في F حيث إن المساواة والجمع والضرب لعنصر من الحقل معرّفة عن طريق المركبات a_i . برهن على أن V فضاء متجهات على F .

(ب) لتكن W المجموعة $\{(a_1,\ldots,a_n,\ldots)\in V \mid \lim_{n\to\infty} a_n=0\}$. برهن على أن W فضاء جزئي من V .

(جـ) لتكن $U=\{(a_1,\ldots,a_n,\ldots)\in V \mid \sum_{i=1}^{\infty} a_i^2<\infty\}$. برهن على أن U فضاء جزئي من V وأنه محتوى في W .

٦ - إذا كان V,U فضائي متجهات على F فعرّف عمليتي الجمع والضرب بعنصر من الحقل في $Hom(U,V)$ كي تكون $Hom(U,V)$ فضاء متجهات على F .

*٧ - باستعمال نتيجة المسألة ٦ برهن على أن $Hom(F^{(n)},F^{(m)})$ يماثل فضاء المتجهات $F^{(nm)}$.

٨ - إذا كان $n>m$. فبرهن على أنه يوجد تشاكل من $F^{(n)}$ على $F^{(m)}$ نواته W تماثل $F^{(n-m)}$.

٩ - إذا كان $v\neq 0$ في $F^{(n)}$. فبرهن على أنه يوجد عنصر T في $Hom(F^{(n)},F)$ بحيث $vT\neq 0$.

١٠ - برهن على وجود تماثل من $F^{(n)}$ إلى $Hom\,(Hom\,(F^{(n)},F),F)$

١١ - إذا كان W,U فضائيين جزئيين من V . فبرهن على أن $U+W=\{v\in V \mid v=u+w, u\in U, w\in W\}$ فضاء جزئي في V .

١٢ - برهن على أن تقاطع فضائين جزئيين من V هو فضاء جزئي من V .

١٣ - إذا كان B,A فضائيين جزئيين من V فبرهن على أن $(A+B)/B$ يماثل $A/(A\cap B)$.

١٤ ـ إذا كان T تشاكلاً من U على V نواته W . فبرهن على وجود تقابل أحادي بين الفضاءات الجزئية من V والفضاءات الجزئية من U التي تحوي W .

١٥ ـ ليكن V فضاء متجهات على $V_1,\ldots,V_n,F$ فضاءات جزئية من V . ولنفرض أن $V=V_1+V_2+\ldots+V_n$ (انظر مسألة ١١) وأن $V_i\cap(V_1+\ldots+V_{i-1}+V_{i+1}+\ldots+V_n)=(0)$ لكل $i=1,2,\ldots,n$. برهن على أن V هو الجمع المباشر الداخلي للفضاءات الجزئية $V_1,\ldots,V_n$.

١٦ ـ ليكن $V=V_1\oplus\ldots\oplus V_n$. برهن على أن V يحوي فضاءات جزئية $\bar{V}_i$ تماثل V_i بحيث أن V يساوي الجمع المباشر الداخلي للفضاءات $\bar{V}_i$.

١٧ ـ لنعرف T على $F^{(2)}$ بواسطة $(x_1,x_2)T=(\alpha x_1+\beta x_2,\gamma x_1+\delta x_2)$ حيث إن $\alpha,\beta,\gamma,\delta$ عناصر ثابتة في F .

(ا) برهن على أن T تشاكل من $F^{(2)}$ إلى نفسه .

(ب) أوجد شروطاً ضرورية وكافية على $\alpha,\beta,\gamma,\delta$ كي تجعل T تماثلاً .

١٨ ـ لنعرِّف T على $F^{(3)}$ بواسطة

$$(x_1,x_2,x_3)T=(\alpha_{11}x_1+\alpha_{12}x_2+\alpha_{13}x_3,\quad \alpha_{21}x_1+\alpha_{22}x_2+\alpha_{23}x_3,\quad \alpha_{31}x_1+\alpha_{32}x_2+\alpha_{33}x_3)$$

أثبت أن T تشاكل من $F^{(3)}$ إلى نفسه وعين شروطاً ضرورية وكافية على α_{ij} كي تكون T تماثلاً .

١٩ ـ ليكن T تشاكلا من V إلى W . باستعمال T عرف تشاكلاً T^* من Hom (W,F) إلى Hom (V,F) .

٢٠ ـ (ا) برهن على أن $F^{(1)}$ لا يماثل $F^{(n)}$ لقيم $n>1$.

(ب) برهن على أن $F^{(2)}$ لا يماثل $F^{(3)}$.

٢١ ـ إذا كان V فضاء متجهات على **حقل غير منته** (infinite field) F . فبرهن على أنه ليس بالإمكان كتابة V كاتحاد مجموعات لعدد منتهٍ من فضاءات جزئية فعلية .

(٤ ـ ٢) الاستقلال الخطي والأساسات

إذا تفحصنا المثالين (٤-١-٤) و(٤-١-٣) المذكورين في البند السابق نلاحظ أنه

بالرغم من وجود العديد من الخواص المشتركة بينهما فإنه يوجد فرق رئيس بين الإثنين. هذا الفرق يبدو في الحقيقة أنه في المثال (٤-١-٤) يمكننا إيجاد عدد منتهٍ من العناصر $1, x, x^2, \ldots, x^{n-1}$ بحيث يمكن كتابة كل عنصر كتركيب من هذه العناصر بمعاملات من F . بينما لا توجد مثل هذه المجموعة المنتهية من العناصر في المثال (٤-١-٣).

الآن نريد أن ندرس، بشيء من التفصيل فضاءات المتجهات التي يمكن توليدها بواسطة مجموعة منتهية من العناصر كما هي الحال في مثال (٤-١-٤).

تعريف

إذا كان V فضاء متجهات على F و $v_1, \ldots, v_n$ في V فيدعى العنصر الذي على الشكل $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ حيث α_i في F تركيب خطي (linear combination) على F للعناصر $v_1, \ldots, v_n$.

إننا سنعمل على حقل ثابت F ونستعمل في أغلب الأحيان عبارة تركيب خطي بدلاً من تركيب خطي على F . كذلك سنكتفي بعبارة فضاء متجهات للدلالة على فضاء متجهات على F .

تعريف

إذا كانت S مجموعة جزئية غير خالية من فضاء المتجهات V فإن التوليد الخطي (linear span) L(S) من المجموعة S هو مجموعة جميع التركيبات الخطية لمجموعات منتهية من عناصر S .

في الحقيقة إننا وضعنا في L(S) جميع العناصر التي تتطلبها شروط فضاء المتجهات، لذا فإنه ليس من الغريب أن نجد التمهيدية الآتية:

تمهيدية (٤-٢-١)

L(S) فضاء جزئي من V .

البرهان

إذا كان w,v في $L(S)$ فإن $v=\lambda_1 s_1+\ldots+\lambda_n s_n$ و $w=\mu_1 t_1+\ldots+\mu_m t_m$

حيث λ_i ، μ_j في F و s_i ، t_j في S .

إذا كان α و β في F فإن

$$\alpha v+\beta w=\alpha(\lambda_1 s_1+\ldots+\lambda_n s_n)+\beta(\mu_1 t_1+\ldots+\mu_m t_m)$$
$$=(\alpha\lambda_1)S_1+\ldots+(\alpha\lambda_n)s_n+(\beta\mu_1)t_1+\ldots+(\beta\mu_m)t_m$$

مما يجعل $\alpha v+\beta w$ في $L(S)$ وبذا يكون $L(S)$ فضاءاً جزئياً من V .

إن البرهان على أجزاء التمهيدية التالية سهل جدًّا نتركه كتمرين للقاريء.

تمهيدية (٤-٢-٢)

إذا كانت T,S مجموعتين جزئيتين من V ، فإن

١ - $S\subset T$ *يقتضي أن* $L(S)\subset L(T)$.

٢ - $L(S\cup T) = L(S)+L(T)$

٣ - $L(L(S)) = L(S)$.

تعريف

يقـال عن فضـاء المتجهات V ***إنه مُنتهى البعد*** *finite-dimensional (على F) إذا وُجدت مجموعة جزئية منتهية S في V بحيث إن $V=L(S)$.*

لاحظ أن $F^{(n)}$ مُنتهِ البعد على F لأنه إذا كانت S تحتوي على المتجهات
$(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots,0,1)$ فإن $V=L(S)$

بالرغم من أننا عرفنا المقصود بفضاء المتجهات مُنتهى البعد فإننا لم نعرف معنى البعد لفضاء المتجهات. هذا ما سنفعله قريبا.

تعريف

إذا كان V فضـاء متجهـات، نقـول إن $v_1,\ldots,v_n$ في V إنها ***مرتبـطة خطيـا***

(linearly dependent) على F إذا وُجِدَت عناصر $\lambda_1,\ldots,\lambda_n$ في F ليس جميعها أصفاراً بحيث إن $\lambda_1 v_1+\lambda_2 v_2+,\ldots,+\lambda_n v_n=0$.

إذا لم تكن المتجهات $v_1,\ldots,v_n$ مرتبطة خطيا على F فيقال إنها **مستقلة خطياً** (linearly independent) على F ، وهنا أيضا سوف نختصر العبارة «مرتبطة خطياً على F » إلى «مرتبطة خطيا». لاحظ أنه إذا كانت $v_1,\ldots,v_n$ مستقلة خطياً فلا يمكن لأحدها أن يساوي صفراً ذلك أنه لو كان $v_1=0$ ، على سبيل المثال، فإن:

$\alpha v_1+0v_2+\ldots+0v_n=0$ لكل $\alpha\neq 0$ في F .

في $F^{(3)}$ من السهولة التحقق من أن (1,0,0) ، (0,1,0) و (0,0,1) مستقلة خطيا بينما (1,1,0) ، (3,1,3) و (5,3,3) مرتبطة خطياً.

نود أن نشير إلى أن الاستقلال الخطي لا يعتمد على المتجهات فحسب ولكن على الحقل أيضا. فعلى سبيل المثال، حقل الأعداد المركبة يعتبر فضاء متجهات على حقل الأعداد الحقيقية وهو أيضا فضاء متجهات على حقل الأعداد المركبة. العنصران $v_1=1$ و $v_2=i$ مستقلان خطياً على الأعداد الحقيقية ولكنهما مرتبطان خطياً على الأعداد المركبة لأن $iv_1 + (-1)v_2 = 0$

إن مفهوم الارتباط الخطي أساسي ومهم جداً في دراستنا هذه. لذا يجدر بنا النظر إلى بعض خصائصه.

تمهيدية (٤-٢-٣)

إذا كانت $v_1,\ldots,v_n$ مستقلة خطياً فإن كل عنصر في توليدها الخطي له تمثيل وحيد على الشكل $\lambda_1 v_1+\ldots+\lambda_n v_n$ حيث λ_i في F .

البرهان

بالتعريف. كل عنصر في التوليد الخطي هو على الشكل $\lambda_1 v_1+\ldots+\lambda_n v_n$.

كي نبين أن هذا التمثيل وحيد يجب أن نثبت أن

$$\lambda_1 v_1+\ldots+\lambda_n v_n=\mu_1 v_1+\ldots+\mu_n v_n$$

تقتضي أن $\lambda_1=\mu_1$ ، $\lambda_2=\mu_2$ ، ... $\lambda_n=\mu_n$. ولكن إذا كان

$$\lambda_1 v_1+\ldots+\lambda_n v_n=\mu_1 v_1+\ldots+\mu_n v_n$$

فإننا نحصل على

$(\lambda_1-\mu_1)v_1+(\lambda_2-\mu_2)v_2+\ldots+(\lambda_n-\mu_n)v_n=0$ والتي تؤدي بالاستعانة بالاستقلال الخطي للعناصر $v_1,\ldots,v_n$ إلى $\lambda_1-\mu_1=0, \lambda_2-\mu_2=0 \ldots \lambda_n-\mu_n=0$.

إن المبرهنة التالية بالرغم من سهولتها وطبيعتها الخاصة تعتبر مهمة جداً ذلك لأن نتائجها تكوِّن أسس الموضوع الذي ندرسه. وسندرج بعض هذه النتائج بعد المبرهنة أما الباقي فسيظهر في التمهيديات والمبرهنات بعد ذلك.

مبرهنة (٤-٢-١)

إذا كانت $v_1,\ldots,v_n$ في V فإنها إما أن تكون مستقلة خطياً أو أن أحد المتجهات v_k هو تركيب خطي من المتجهات التي تسبقه $v_1,\ldots,v_{k-1}$.

البرهان

إذا كانت $v_1,\ldots,v_n$ مستقلة خطياً فليس هناك ما يدعو للبرهان. لذا نفرض أن $\alpha_1 v_1+\ldots+\alpha_n v_n=0$ حيث ليس كل α_i تساوي صفراً. ليكن k أكبر عدد صحيح بحيث $\alpha_k\neq 0$. لما كان $\alpha_i=0$ لقيم $i>k$ فإن $\alpha_1 v_1+\ldots+\alpha_k v_k=0$ والذي يقتضي أن :

$$v_k=\alpha_k^{-1}(-\alpha_1 v_1-\alpha_2 v_2-\ldots-\alpha_{k-1}v_{k-1})=(-\alpha_k^{-1}\alpha_1)v_1+\ldots+(-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$$

لأن $\alpha_k\neq 0$. لذا نجد أن v_k هو تركيب خطي من المتجهات التي تسبقه.

نتيجة (١)

إذا كانت $v_1,\ldots,v_n$ في V تولد W خطياً وكانت $v_1,\ldots,v_k$ مستقلة خطيا فإن بإمكاننا

إيجـاد مجمـوعـة جزئية من $v_1,\dots,v_n$ على الصيغة $v_1,v_2,\dots,v_k,v_{i_1},\dots,v_{i_r}$ تحوي عناصر مستقلة خطياً والتي توليدها الخطي يساوي W أيضا .

البرهان

إذا كانت $v_1,\dots,v_n$ مستقلة خطياً فلا يوجد ما يدعو للبرهان . وفيما عدا ذلك تَخَلَّص من أول عنصر v_j يساوي تركيباً خطياً لسابقيه . لأن $v_1,\dots,v_k$ مستقلة خطياً فإن $j>k$. لذا نحصل على المجموعة الجزئية $v_1,\dots,v_k,\dots,v_{j-1},v_{j+1},\dots,v_n$ التي تحوي $n-1$ من العناصر. من الواضح أن توليدها الخطي مُحْتَوى في W ، ولكننا ندعي أنه في الحقيقة يساوي W . لأنه إذا كان w في W فإنه يمكن كتابته كتركيب خطي من $v_1,\dots,v_n$. ولكن في ذلك التركيب الخطي يمكننا استبدال v_j بتركيب خطي من $v_1,\dots,v_{j-1}$ مما يؤدي إلى أن w هو تركيب خطي من $v_1,\dots,v_{j-1},v_{j+1},\dots,v_n$.

بالاستمرار في التخلص من العناصر التي تساوي تركيباً خطياً لسابقيها ، نصل إلى مجموعة جزئية $v_1,\dots,v_k,v_{i_1},\dots,v_{i_r}$ توليدها الخطي يساوي W . ولكن لا يوجد عنصر فيها يساوي تركيبا خطياً لسابقيه . وفقاً للمبرهنة (٤-٢-١) تكون العناصر $v_1,\dots,v_k,v_{i_1},\dots,v_{i_r}$ مستقلة خطياً .

نتيجة (٢)

إذا كان V فضاء متجهات مُنتهى البعد فإنه يحوي مجموعة منتهية $v_1,\dots,v_n$ من العناصر المستقلة خطياً والتي توليدها الخطي يساوي V .

البرهان

لما كان V منتهي البعد فإنه توليد خطي لعدد منته من العناصر $u_1,\dots,u_m$. وفقاً للنتيجة (١) يمكننا إيجاد مجموعة جزئية من هذه العناصر ونرمز لعناصرها بالرموز $v_1,\dots,v_n$ بحيث إنها مستقلة خطياً وتوليدها الخطي يساوي V .

تعريف

تُدعى المجموعة الجزئية S من فضاء المتجهات V أساساً (basis) للفضاء V إذا كانت عناصر S مستقلة خطياً (بمعنى أن أي عدد منته من عناصر S مستقل خطياً) و $V=L(S)$.

بهذه التسمية، يمكننا أن نستبدل نتيجة (٢) بما يلي :

نتيجة (٣)

إذا كان V فضاء متجهات منتهي البعد وكانت المتجهات $v_1,\ldots,v_m$ تولد V فإن مجموعة جزئية من $v_1,\ldots,v_m$ تكون أساساً للفضاء V .

إن النتيجة (٣) تؤكد أن فضاء المتجهات المنتهي البعد له أساس يحوي عدداً منتهياً من العناصر $v_1,\ldots,v_n$. وبالاستعانة بتمهيدية (٤-٢-٣) نستنتج أن كل عنصر في V له تمثيل وحيد على الشكل $\alpha_1 v_1+\ldots+\alpha_n v_n$ حيث $\alpha_1,\ldots,\alpha_n$ في F .

الآن لننظر إلى بعض الاستنتاجات التي يمكننا استخلاصها من الملاحظتين السابقتين. لنفرض أن V هو فضاء متجهات منتهي البعد على F، كما رأينا سابقا V له أساس $v_1,\ldots,v_n$. لذا أي عنصر في V له تمثيل وحيد على الصيغة $v=\alpha_1 v_1+\ldots+\alpha_n v_n$. لنعرف تطبيقاً من V إلى $F^{(n)}$ يجعل صورة $\alpha_1 v_1+\ldots+\alpha_n v_n$ تساوي $(\alpha_1,\ldots,\alpha_n)$. بسبب وحدانية التمثيل بهذه الصيغة فإن التطبيق يكون حسن التعريف، أحاديا وغامراً ويمكن إثبات أنه يحقق جميع خواص التماثل. لذا فإن V يماثل $F^{(n)}$ لعدد صحيح ما n حيث إن n هو، في الحقيقة، عدد العناصر في أساس ما للفضاء V على F . لو كان للفضاء V أساس آخر يحوي m من العناصر لكان V يماثل $F^{(m)}$ للأسباب السابقة نفسها. هذا يجعل $F^{(m)},F^{(n)}$ متماثلين لأن كلا منهما يماثل V .

مما سبق يبرز السؤال التالي: تحت أي شروط على m,n يكون $F^{(m)}, F^{(n)}$ متماثلين؟

إن إدراكنـا يدعـونـا للاعتقـاد بأن هذا ممكن فقط في حالة n=m . فلو كان F حقلاً فيه عدد منته من العناصر ـ مثل Z_p (الأعـداد الصحيحـة قياس العدد الأولي p) فإن $F^{(n)}$ يحوي p^n من العناصر بينما يحوي $F^{(m)}$ على p^m من العناصر. ولكن التماثل يقتضي أنهما يحويان العدد نفسه من العناصر ولذا يكون n=m . ومن وجهة نظر أخرى لو كان F حقل الأعداد الحقيقية فإن $F^{(n)}$ (وهذه الطريقة الهندسية قد تكون غامضة للقارىء) يمثل الفضاء الحقيقي ذا البعد n وإحساسنا الهندسي يخبرنا أن الفضاء ذا البعد n يختلف عن الفضاء ذا البعد m إذا كان $n \neq m$. لذا يمكننا التوقع أنه إذا كان F حقلا ما فإن $F^{(n)}$ يماثل $F^{(m)}$ فقط في حالة n=m .

بصورة مكافئة ومما سبق ذكره نتوقع أن أي أساسين للفضاء V يحويان العدد نفسه من العناصر، ومن أجل ذلك نبرهن على التمهيدية التالية.

تمهيدية (٤-٢-٤)

إذا كان $v_1,\ldots,v_n$ أساساً للفضاء V على F وكانت $w_1,\ldots,w_m$ في V مستقلة خطيا على F فإن $m \leq n$.

البرهان

كل متجه في V وعلى وجه الخصوص w_m هو تركيب خطي من $v_1,\ldots,v_n$. لذا فإن المتجهات $w_m,v_1,\ldots,v_n$ مرتبطة خطيا وفضلا عن ذلك فإنها تولد V لأن $v_1,\ldots,v_n$ تولد V بحد ذاتها. إذن توجد مجموعة جزئية فعلية من $w_m,v_{i_1},\ldots,v_{i_k}$ حيث $k \leq n-1$ تكون أساساً للفضاء V . بهذا نكون قد استبدلنا أحد العناصر v_i على الأقل بالعنصر w_m في تكوين هذا الأساس الجديد. كرر العملية السابقة مع المجموعة $w_{m-1},w_m,v_{i_1},\ldots,v_{i_k}$. باستعمال نتيجة (١) من مبرهنة (٤-٢-١) يمكننا استخراج أساس على الشكل $w_{m-1},w_m,v_{j_1},\ldots,v_{j_s}$ حيث $s \leq n-2$. بالاستمرار على هذا المنوال نحصل على أساس للفضاء V على الشكل $w_2,\ldots,w_{m-1},w_m,v_\alpha,v_\beta,\ldots$. ولما كان

w_1 لا يساوي تركيباً خطياً من $w_2,\ldots,w_{m-1}$ فلا بد للأساس السابق أن يحتوي على متجه من الشكل v_s . لاحظ أنه في ذلك الأساس استخدمنا $m-1$ من العناصر $w_2,\ldots,w_{m-1},w_m$ وفي الوقت نفسه تخلينا عن $m-1$ من العناصر على الصيغة v_t ومع ذلك بقي عنصر من الصيغة v_s . لذا $m-1\leqslant n-1$ مما يؤدي إلى أن $m\leqslant n$.

هذه التمهيدية تعطينا نتائج (ندرجها فيما يلي) تمثل حقائق أساسية تعيننا على فهم طبيعة بعد فضاء المتجهات. هذه النتائج ذات أهمية عظمى في كل ما سيأتي ليس في هذا الفصل فحسب بل في بقية هذا الكتاب وبالأحرى في جميع مادة الرياضيات. إن هذه النتائج تعتبر مبرهنات بحد ذاتها.

نتيجة (١)

إذا كان V فضاء متجهات منتهى البعد على F فإن أي أساسين في V لهما العدد نفسه من العناصر.

البرهان

ليكن $v_1,\ldots,v_n$ أساساً للفضاء V على F و $w_1,\ldots,w_m$ أساساً آخر. لذا فإن $w_1,\ldots,w_n$ مستقلة خطياً على F وبناءاً علي ووفقا لتمهيدية (٤-٢-٤) نحصل على $m\leqslant n$. باستبدال دور الأساسين السابقين فيما بينهما نحصل على $n\leqslant m$ مما يؤدي إلى أن $n=m$.

نتيجة (٢)

يكون $F^{(n)}$ مماثلا للفضاء $F^{(m)}$ إذا وفقط إذا كان $n=m$.

البرهان

يحوي الفضاء $F^{(n)}$ كأحد أُسُسه مجموعة المتجهات $(1,0,\ldots,0)$ ، $(0,1,\ldots,0)$ ، . . . ، $(0,0,\ldots,1)$ الحاوية على n من العناصر. كذلك الفضاء

يحوي $F^{(m)}$ أساساً له m من العناصر. إن أي تماثل من فضاء متجهات إلى آخر يأخذ أساساً للفضاء الأول إلى أساس للفضاء الثاني (انظر مسألة ٤ في نهاية هذا البند) ولذا فإن n=m وفقاً للنتيجة ١.

إن النتيجة (٢) تؤكد أن ما استنتجناه بأنفسنا فيما سبق حول إمكانية تماثل $F^{(n)}, F^{(m)}$ هو صحيح من الناحية الرياضية. ولقد ذكرنا حينئذ أن V يماثل $F^{(n)}$ لعدد ما n . وفقاً للنتيجة ٢ فإن العدد n وحيد وهكذا يكون لدينا.

نتيجة (٣)

إذا كان V فضاء متجهات منتهي البعد على F فإن V يماثل $F^{(n)}$ لعدد صحيح وحيد n ، وفي الحقيقة أن n يساوي عدد العناصر في أي أساس للفضاء V على F .

تعريف

يطلق على العدد الصحيح n في نتيجة (٣) ***بعد (dimension)*** *فضاء المتجهات V على F .*

إن بعد الفضاء V على F هو بالأحرى عدد العناصر في أساس من V على F .

سوف نرمز لبعد V على F بالرمز dim V وعندما نريد أن نؤكد دور الحقل F تكتب $\dim_F V$.

نتيجة (٤)

أي فضائي متجهات منتهيي البعد على F ولهما البعد نفسه يكونان متماثلين.

البرهان

إذا كان البعد هو n فإن أيًّا من الفضاءين يماثل $F^{(n)}$ وبالتالي يكونان متماثلين.

والآن نسأل: ما مدى الحرية التي نملكها كي ننشيء أساساً لفضاء متجهات V ؟ إن التمهيدية التالية تؤكد أنه إذا بدأنا من أية مجموعة من المتجهات المستقلة خطياً يمكننا توسيع هذه المجموعة لتكون أساساً للفضاء V .

تمهيدية (٤-٢-٥)

إذا كان V فضاء متجهات منتهي البعد على F و $u_1,\dots,u_m$ في V مستقلة خطياً فإن بإمكاننا إيجاد متجهات $u_{m+1},\dots,u_{m+r}$ في V بحيث $u_1,\dots,u_m,u_{m+1},\dots,u_{m+r}$ تكون أساساً للفضاء V .

البرهان

بما أن V مُنتهى البعد فإن له أساساً يحوي عدداً منتهيا من العناصر $v_1,\dots,v_n$. وحيث إن هذه العناصر تولد V فإن المتجهات $u_1,\dots,u_m,v_1,\dots,v_n$ تولد V أيضاً. ووفقا لنتيجة (١) من مبرهنة (٤-٢-١) توجد مجموعة جزئية من تلك المتجهات على الصيغة $u_1,\dots,u_m,v_{i_1},\dots,v_{i_r}$ تحوي عناصر مستقلة خطياً وتولد V . لبرهان التمهيدية إجعل $u_{m+1}=v_{i_1}$ ، . . . ، $u_{m+r}=v_{i_r}$

إن التمهيدية التالية تجيب على السؤال: ما هي العلاقة بين بعد فضاء المتجهات V وبعد صورة تشاكل من V ؟

تمهيدية (٤-٢-٦)

إذا كان V منتهي البعد و W فضاءاً جزئياً من V فإن W مُنتهى البعد أيضاً و $\dim W \leq \dim V$ كذلك $\dim V/W = \dim V - \dim W$.

البرهان

إذا كان $n=\dim V$ فوفقا لتمهيدية (٤-٢-٤) أي $n+1$ من العناصر في V يجب أن تكون مرتبطة خطياً، وعلى وجه الخصوص أي $n+1$ من العناصر في W مرتبطة

خطياً. لذا يمكننا إيجاد مجموعة لا يمكن الزيادة عليها من العناصر المستقلة خطياً في W مثل $w_1,\dots,w_m$ ويجب أن يكون $m\leqslant n$. إذا كان w في W فإن المتجهات $w_1,\dots,w_m,w$ مرتبطة خطياً، أي أنه توجد عناصر $\alpha,\alpha_1,\dots,\alpha_m$ في F ليست كلها صفراً بحيث إن:

$$\alpha w+\alpha_1 w_1+\dots+\alpha_m w_m=0$$

إذا كان $\alpha=0$ فإن الاستقلال الخطي للعناصر w_i يعطينا $\alpha_i=0$ ، $1\leqslant i\leqslant m$ وهذا تناقض. لذا $\alpha\neq 0$ و $w=-\alpha^{-1}(\alpha_1 w_1+\dots+\alpha_m w_m)$. ونتيجة لذلك تولد المتجهات $w_1,\dots,w_m$ الفضاء الجزئي W مما يجعل W مُنتهي البعد على F وله أساس يحوي على m من العناصر حيث $m\leqslant n$. لذا $\dim W\leqslant \dim V$ وذلك من تعريف البعد لفضاء المتجهات.

الآن ليكن $w_1,\dots,w_m$ أساساً للفضاء الجزئي W . وبالاستعانة بتمهيدية (٤-٢-٥) يمكننا توسيع هذا الأساس إلى أساس $w_1,\dots,w_m,v_1,\dots,v_r$ للفضاء V حيث $m=\dim W$, $m+r=\dim V$.

لتكن $\bar{v}_1,\dots,\bar{v}_r$ صور العناصر $v_1,\dots,v_r$ في $\bar{V}=V/W$. وحيث إن أي متجه v في V هو على الصيغة:

$$v=\alpha_1 w_1+\dots+\alpha_m w_m+\beta v_1+\dots+\beta_r v_r$$

فإن $\bar{v}$ ، صورة v ، هي على الصيغة:

$$\bar{v}=\beta_1\bar{v}_1+\dots+\beta_r\bar{v}_r$$

(لأن $\bar{w}_1=\bar{w}_2=\dots=\bar{w}_m=0$).

لذا فإن $\bar{v}_1,\dots,\bar{v}_r$ تولد V/W وزيادة على ذلك ندعي أنها مستقلة خطياً.

فلو كان $\gamma_1\bar{v}_1+\dots+\gamma_r\bar{v}_r=0$

فإن $\gamma_1 v_1+\dots+\gamma_r v_r$ في W مما يجعل $\gamma_1 v_1+\dots+\gamma_r v_r=\lambda_1 w_1+\dots+\lambda_m w_m$ وهذا يؤدي إلى أن $\gamma_1=\dots=\gamma_r=\lambda_1=\dots=\lambda_m=0$ ذلك لأن المتجهات $w_1,\dots,w_m,v_1,\dots,v_r$ مستقلة خطياً. هكذا بينا أن V/W له أساس يحوي r من العناصر وبناءً عليه يكون

$$\dim V/W = r = \dim V - m = \dim V - \dim W$$

نتيجة

إذا كان B,A فضاءين جزئيين منتهيي البعد من فضاء المتجهات V ، فإن $A+B$ منته البعد و $\dim(A+B) = \dim(A) + \dim(B) - \dim(A \cap B)$

البرهان

بالاستعانة بمسألة (١٣) في نهاية بند (٤-١) نحصل على

$$\frac{A+B}{B} \approx \frac{A}{A \cap B}$$

وحيث إن B,A منتهيي البعد يكون

$$\dim(A+B) - \dim B = \dim\left(\frac{A+B}{B}\right) = \dim\left(\frac{A}{A \cap B}\right) = \dim A - \dim(A \cap B)$$

بنقل الحدود نحصل على الصيغة المذكورة في النتيجة.

مسائل

١ - برهن تمهيدية (٤-٢-٢)

٢ - (أ) إذا كان F حقل الأعداد الحقيقية. فبرهن على أن المتجهات $(1,1,0,0)$ ، $(0,1,-1,0)$ و $(0,0,0,3)$ في $F^{(4)}$ مستقلة خطياً على F .

(ب) ما هي الشروط على مميز الحقل F كي تكون المتجهات الثلاثة في (أ) مرتبطة خطياً؟

٣ - إذا كان للفضاء V أساساً يحوي n من العناصر. فبرهن وبصورة مفصلة على أن V يماثل $F^{(n)}$.

٤ - إذا كان T تماثلا من V على W . وكان S أساساً في V فأثبت أن $T(S)$ أساس في W .

٥ - إذا كان V منتهي البعد و T تماثل من V إلى V . فبرهن على أن T يجب أن يكون غامراً.

٦ ـ إذا كان V منتهي البعد و T تشاكل من V على V . فبرهن على أن T يجب أن يكون أحادياً وبالتالي تماثلا .

٧ ـ إذا كان بعد الفضاء V يساوي n . فأثبت أن أية مجموعة عناصرها n من المتجهات المستقلة خطيا في V تكوِّن أساساً للفضاء V .

٨ ـ إذا كان V منتهي البعد و W فضاءاً جزئياً من V بحيث $\dim V=\dim W$. فبرهن على أن $V=W$.

٩ ـ إذا كان V منتهي البعد و T تشاكلا غير غامر من V إلى نفسه . فبرهن على أنه يوجد $v\neq 0$ في V بحيث $vT=0$.

١٠ ـ ليكن F حقلا و $F[x]$ فضاء كثيرات الحدود في x على F . برهن على أن $F[x]$ ليس منتهي البعد على F .

١١ ـ ليكن V_n حيث

$$V_n=\{p(x)\in F[x]\,|\,\deg p(x)<n\}$$

وعرف T على النحو

$$(\alpha_0+\alpha_1x+\ldots+\alpha_{n-1}x^{n-1})T=\alpha_0+\alpha_1(x+1)+\alpha_2(x+1)^2+\ldots+\alpha_{n-1}(x+1)^{n-1}$$

برهن على أن T تماثل من V_n على نفسه .

١٢ ـ لتكن W هي المجموعة

$$\{\alpha_0+\alpha_1x+\ldots+\alpha_{n-1}x^{n-1}\in F[x]\ |\alpha_0+\alpha_1+\ldots+\alpha_{n-1}=0\}$$

برهن على أن W فضاء جزئي من V_n وأوجد أساساً له على الحقل F .

١٣ ـ ليكن $v_1,\ldots,v_n$ أساساً للفضاء V و $w_1,\ldots,w_n$ أي n من العناصر في V وعرف T على V بالشكل التالي : $(\lambda_1v_1+\ \ldots+\lambda_nv_n)T=\lambda_1w_1+\ldots+\lambda_nw_n$

(ا) أثبت أن T تشاكل من V إلى نفسه .

(ب) متى يكون T تماثلاً؟

١٤ ـ برهن على أن أي تشاكل من V إلى نفسه حيث V منتهي البعد هو على الشكل المذكور في مسألة (١٣) وذلك باختيارنا لعناصر مناسبة $w_1,\ldots,w_n$.

١٥ ـ عودة إلى مسألة (١٣)، لما كان $v_1,\ldots,v_n$ أساساً للفضاء V فإن كل w_i يساوي $\alpha_{i1}v_1+\ldots+\alpha_{in}v_n$ حيث α_{ij} في F . بين أن العناصر α_{ij} في F والتي عددها n^2 تعين التشاكل T .

١٦* ـ إذا كان $\dim_F V=n$. فبرهن على أن $\dim_F(Hom(V,V))=n^2$.

١٧ ـ إذا كان V منتهي البعد و W فضاءًا جزئياً من V . فبرهن على أنه يوجد فضاء جزئي W_1 في V بحيث $V=W\oplus W_1$

(٣ ـ ٤) الفضاءات الثنوية

ليكن V و W فضائي متجهات على حقل F . سبق أن عرفنا Hom(V,W) على أنه مجموعة جميع التشاكلات من V إلى W ولكننا لم نعرف بعد أية بنية جبرية على هذه المجموعة . الآن نهم بتعريف عمليتين على Hom(V,W) كي نجعل منها فضاء متجهات على F . في الحقيقة أننا قد نوهنا بكيفية تعريف العمليتين عند تقديمنا لبعض المسائل في البندين السابقين بيد أننا نريد معالجة الموضوع ضمن سياق المادة .

ليكن T,S عنصرين في Hom(V,W) وهذا يعني أن كلا منهما تشاكل من V إلى W . وبالعودة إلى تعريف مثل هذا التشاكل نجد أن $(v_1+v_2)S=v_1S+v_2S$ و $(\alpha v_1)S=\alpha(v_1S)$ لجميع v_1,v_2 في V و α في F ، وكذلك الحال بالنسبة للتشاكل T .

أولاً : تعرف عملية جمع للعنصرين S و T في Hom(V,W) بالطريقة التالية :

$$v(S+T)=vS+vT$$

لكل v في V .

يجب التحقق من أن S+T في Hom(V,W) ومن أجل ذلك ليكن v_1,v_2 في V فنحصل على

$(v_1+v_2)(S+T)=(v_1+v_2)S+(v_1+v_2)T$ ، ولما كان $(v_1+v_2)S=v_1S+v_2S$

و $(v_1+v_2)T=v_1T+v_2T$ ولما كانت عملية الجمع في W إبدالية، لذا نجد

$S+T$ ومـرة أخـرى نسـتـعـيد تعـريف $(v_1+v_2)(S+T)=v_1S+v_1T+v_2S+v_2T$ فيصبـح الجـانب الأيمن من المسـاواة $v_1(S+T)+v_2(S+T)$ وبـذلـك نكـون قد أثبـتنـا أن $(v_1+v_2)(S+T)=v_1(S+T)+v_2(S+T)$ وبصـورة مشـابهـة نجـد أن $(\alpha v)(S+T)=\alpha(v(S+T))$.

فنستنتج أن $S+T$ في $Hom(V,W)$. ليكن O التشـاكـل من V إلى W الذي يرسل كل عنصر في V إلى العنصر الصفـري في W و $S-$ لعنصر S في $Hom(V,W)$ يعـرف بالطريقة $v(-S)=-(vS)$. الآن من السهل التحقق من أن $Hom(V,W)$ زمرة إبدالية بالنسبة لعملية الجمع أعلاه.

الآن نعـرف λS حيث λ في F و S في $Hom(V,W)$ بالـطريقـة الـتـالـية $v(\lambda S)=\lambda(vS)$ لجميع v في V . نترك للقـارىء التـأكـد من أن λS في $Hom(V,W)$ وأن $Hom(V,W)$ فضاء متجهات على F بالنسبة إلى العمليتين المعرفتين عليه. ولكن يجب أن نعي أننا حتى الآن لا يمكن أن نضمن وجود أي عنصر في $Hom(V,W)$ ما عدا التشاكل الصفري. وعلى أية حال نكون قد برهنا التمهيدية التالية.

تمهيدية (٤-٣-١)

إن $Hom(V,W)$ فضاء متجهات على F بالنسبة إلى العمليتين المعرفتين أعلاه.

إن مثل النتيجة المذكورة في تمهيدية (٤-٣-١) في الحقيقة تعطينا معلومات قليلة جداً وأنها بالأحرى مجرد تأكيد بأن التعريفين اللذين قُدِّما أعلاه صحيحان.

إننا نود أن نحصل على نتائج عن $Hom(V,W)$ تكون أكثر عمقا ومثل هذه ما تذكره المبرهنة التالية.

مبرهنة (٤-٣-١)

إذا كان بُعْـدا V و W على الحـقـل F هما n,m على الـترتـيب فإن بعـد $Hom(V,W)$ على F يساوي mn .

البرهان

سوف نثبت المبرهنة بتقديمنا أساس للفضاء $Hom(V,W)$ على F يحوى mn من العناصر.

ليكن $v_1,\dots,v_m$ أساساً للفضاء V على F و $w_1,\dots,w_n$ أساس W على F . وإذا كان v في V فإن $v=\lambda_1 v_1+\dots+\lambda_m v_m$ حيث $\lambda_1,\dots,\lambda_n$ عناصر معيّنة بصورة وحيدة في F . عرف $T_{ij}:V\to W$ بالطريقة $vT_{ij}=\lambda_i w_j$ ، وبصورة خاصة $v_kT_{ij}=0$ إذا كان $k\neq i$ ، $v_iT_{ij}=w_j$ وذلك من وجهة نظر الأساسين المذكورين أعلاه. إنه لمن السهل التحقق من أن T_{ij} في $Hom(V,W)$ ونترك هذا تمريناً للقارىء. لاحظ أن i يمكن أن يكون أيًا من الأعداد $1,2,\dots,m$ و j من الأعداد $1,2,\dots,n$ وبذا يكون عدد T_{ij} المعرفة أعلاه هو mn .

إننا ندعي أن العناصر T_{ij} تشكل أساساً للفضاء $Hom(V,W)$ على F . ومن أجل ذلك ليكن S في $Hom(V,W)$ وحيث إن v_1S في W وأن أي عنصر في W هو تركيب خطي على F للعناصر $w_1,\dots,w_n$ فإن:

$v_1S=\alpha_{11}w_1+\alpha_{12}w_2+\dots+\alpha_{1n}w_n$ لعناصر $\alpha_{11},\alpha_{12},\dots,\alpha_{1n}$ في F . في الحقيقة

$v_iS=\alpha_{i1}w_1+\alpha_{i2}w_2+\dots+\alpha_{in}w_n$ لكل $i=1,2,\dots,m$

لنعتبر التشاكل

$$S_0=\alpha_{11}T_{11}+\alpha_{12}T_{12}+\dots+\alpha_{1n}T_{1n}+\alpha_{21}T_{21}+\dots+\alpha_{2n}T_{2n}+\dots+$$
$$\alpha_{i1}T_{i1}+\dots+\alpha_{in}T_{in}+\dots+\alpha_{m1}T_{m1}+\dots+\alpha_{mn}T_{mn}$$

ودعنا نحسب v_kS_0 لعنصر الأساس v_k .

$$v_kS_0=v_k(\alpha_{11}T_{11}+\dots+\alpha_{m1}T_{m1}+\dots+\alpha_{mn}T_{mn})=\alpha_{11}(v_kT_{11})+$$
$$\alpha_{12}(v_kT_{12})+\dots+\alpha_{m1}(v_kT_{m1})+\dots+\alpha_{mn}(v_kT_{mn}).$$

وحيث إن $v_kT_{ij}=0$ عندما $i\neq k$ و $v_kT_{kj}=w_j$ يؤول حاصل الجمع إلى $v_kS_0=\alpha_{k1}w_1+\dots+\alpha_{kn}w_n$ والذي يساوي v_kS . لذا فإن التشاكلين S_0 و S يتفقان في قيمهما على أساس من V وهذا يجعل $S_0=S$ (أنظر مسألة (٣) في

نهاية هذا البنــد). ولكن S_0 هو تركيب خطي من العنــاصر T_{ij} مما يؤدي إلى أن S يســاوي التركيب الخــطي نفســه؛ وبــاختصــار فقــد بيّنــا أن العنــاصر $T_{11},T_{12},...,T_{1n},...,T_{m1},...,T_{mn}$ تولد $Hom(V,W)$ على F .

كي نثبت أن العنـاصر أعـلاه تكـون أسـاسـاً للفضـاء $Hom(V,W)$ على F بقي لنا أن نبيّن أنها مستقلة خطياً على F .

لنفرض أن :

$$\beta_{11}T_{11}+\beta_{12}T_{12}+...+\beta_{1n}T_{1n}+...+\beta_{i1}T_{i1}+...+\beta_{in}T_{in}+...+\beta_{m1}T_{m1}+...+\beta_{mn}T_{mn}=0$$

حيث إن جميع β_{ij} في F . بتطبيق هذا على v_k نحصل على

$$0=v_k\ (\beta_{11}T_{11}+...+\beta_{ij}T_{ij}+...+\beta_{mn}T_{mn})=\beta_{k1}w_1+\beta_{k2}w_2+...+\beta_{kn}w_n$$

لأن $v_kT_{ij}=0$ عنــدمــا $i\neq k$ و $v_kT_{kj}=w_j$. ولــكــن $w_1,...,w_n$ مســتــقــلة خطيا على F مما يؤدي إلى أن $\beta_{kj}=0$ لجميع k و j . لذا فإن T_{ij} مستـقـلة خطيا على F مما يجعل منها أساساً للفضاء $Hom(V,W)$ على F .

كنتيجـة مبـاشرة من مبرهنة (٤-٣-١) هي أن $Hom(V,W)$ لا يحوي العنصر الصفــري فقط وذلــك في حالــة $V\neq(0)$ و $W\neq(0)$ لأن بعـد $Hom(V,W)$ على F يساوي mn حيث $mn\geq 1$.

هناك بعض الحالات الخاصة والمهمة في الوقت نفسه من مبرهنة (٤-٣-١) نكتبها على صيغة نتائج .

نتيجة (١)

إذا كان $dim_F V=m$ فإن $dim_F Hom(V,V)=m^2$

البرهان

إجعل $V=W$ في المبرهنة فيكون $m=n$ و $mn=m^2$.

نتيجة (٢)

إذا كان $dim_F V=m$ فإن $dim_F Hom(V,F)=m$

البرهان

إن بعد F كفضاء متجهات على F يساوي 1 . بتطبيق المبرهنة نحصل على

$dim_F Hom(V,F)=m$

إن النتيجة (٢) تؤدي إلى الحقيقة المهمة أنه إذا كان V منتهي البعد على F فإنه يماثل $Hom(V,F)$ ذلك لأن لهما البعد نفسه على F وَفْقاً للنتيجة (٤) من تمهيدية (٤-٢-٤) . إن لهذا التماثل بعض العيوب منها، أنه يعتمد على كون V منتهي البعد على F أي أن هذا التماثل لا يوجد في حالة كون V غير منتهي البعد على F . كما أنه لا توجد بنية محددة لهذا التماثل تصلح لجميع فضاءات المتجهات. إذ أنها تعتمد اعتماداً قويا على الطبيعة الخاصة للفضاء المنتهي البعد. ومن ناحية أخرى سنرى في الصفحات القليلة القادمة أنه يمكن بناء تماثل معين من أي فضاء متجهات V إلى $Hom(Hom(V,F),F)$.

تعريف

*إذا كان V فضاء متجهات فإن **فضاءه الثنوي** (dual space) هو $Hom(V,F)$.*

سوف نستعمل الرمز $\hat{V}$ للدلالة على الفضاء الثنوي للفضاء V كما سنطلق على عنصر من $\hat{V}$ إسم **دالي خطي** من V إلى F .

إذا لم يكن V منتهي البعد على F فإن $\hat{V}$ يكون عادة واسعاً جداً مما لا يجعلنا نكترث به. وعند دراسة الفضاءات غير المنتهية البعد يكون لدينا بناء آخر معرَّف عليها مثل

التبولوجي وكفضاء ثنوي لا نأخذ عادة جميع $\hat{V}$ بل فضاءً جزئياً محدداً منه . وإذا كان V منتهي البعد فإن فضاءه الثنوي $\hat{V}$ يعرف دائما على أنه Hom(V,F) كما ذكرنا ذلك آنفا .

في برهان مبرهنة (٤-٣-١) أنشأنا أساساً للفضاء Hom(V,W) بالاستعانة بأساس محدّد من كل من V و W وهذا الأساس يعتمد كلياً على اختيارنا لأساسي V و W على الترتيب. أي أننا لو غيرنا الأساسين المعنيين لاختلف أساس Hom(V,W) . إنه لمن الأفضل كمبدأ عام أن لا يعتمد البرهان ولا الإنشاء على اختيار أساس فضاء المتجهات، ويشار لمثل هذا البرهان بالقول إنه لا متغير. إن البرهان اللامتغير يتميز بالإضافة إلى الناحية الذوقية على البرهان المعتمد على الأساس بأنه يريحنا من مسألة التدقيق في الأمور المتعلقة باختيارنا للأساس.

إن عناصر $\hat{V}$ هي دوال معرّفة على V قيمها في F . وباتباعنا لرموز الدوال سوف نشير لعناصر $\hat{V}$ بالرموز g,f الخ وإلى قيمة الدالة عند v في V بالرمز f(v) (بدلاً من vf) .

ليكن V فضاء متجهات منتهي البعد على F و $v_1,\ldots,v_n$ أساساً للفضاء V .
نعرِّف $\hat{v}_i$ في $\hat{V}$ على النحو $\hat{v}_i(v_j)=0$ إذا كان $i\neq j$ ، $\hat{v}_i(v_i)=1$
و $\hat{v}_i(\alpha_1 v_1+\ldots+\alpha_i v_i+\ldots+\alpha_n v_n)=\alpha_i$.

في الحقيقة أن $\hat{v}_i$ هي بالأحرى T_{ij} المعرّفة في برهان مبرهنة (٤-٣-١) حيث هنا $W=F$ أحادي البعد على F .

لذا نستنتج أن $\hat{v}_1,\ldots,\hat{v}_n$ تكون أساساً للفضاء $\hat{V}$ ونطلق عليه إسم **الأساس الثنوي** (dual basis) للأساس $v_1,\ldots,v_n$. إذا كان $v\neq 0$ في V فوفقاً لتمهيدية (٤-٢-٥) يمكننا إيجاد أساس على الشكل $v_1=v,v_2,\ldots,v_n$ وبذلك نحصل على عنصر في $\hat{V}$ هو $\hat{v}_1$ بحيث $\hat{v}_1(v_1)=\hat{v}_1(v)=1\neq 0$ وبذلك نكون قد أثبتنا التمهيدية التالية.

تمهيدية (٤-٣-٢)

إذا كان V منتهي البعد و $v\neq 0$ في V ، فيوجد عنصر f في $\hat{V}$ بحيث $f(v)\neq 0$.

في الحقيقة إن تمهيدية (٤-٣-٢) تبقى صحيحة في حالة كون V غير منتهي البعد بيد أننا لا نحتاج هذه النتيجة. ولكون برهانها يتطلب بعض الحقائق المنطقية غير المرتبطة بدراستنا الحالية فسوف لا نتطرق إلى البرهان.

الآن ليكن v_0 في V حيث V فضاء متجهات لا على التعيين على الحقل F . عندما نُثَبِّت v_0 ونجعل f تتغير في $\hat{V}$ فإن $f(v_0)$ تعرف دالياً خطياً من $\hat{V}$ إلى F (لاحظ أننا استبدلنا دور الدالة والمتغير). لنرمز إلى هذه الدالة بالرمز T_{v_0} أي أن $T_{v_0}(f)=f(v_0)$ لكل f في $\hat{V}$. الآن نسأل: ماذا يمكننا القول عن T_{v_0} ؟

أولاً

$$T_{v_0}(f+g)=(f+g)(v_0)=f(v_0)+g(v_0)=T_{v_0}(f)+T_{v_0}(g)$$

ثانياً

$$T_{v_0}(\lambda f)=(\lambda f)(v_0)=\lambda f(v_0)=\lambda T_{v_0}(f)$$

وهكذا نجد أن T_{v_0} تقع في الفضاء الثنوي للفضاء $\hat{V}$ والذي نرمز له بالرمز $\hat{\hat{V}}$ وندعوه **الفضاء الثنوي الثاني** (second dual space) للفضاء V .

إذا كان v في V فبإمكاننا أن نقرن معه العنصر T_v في $\hat{\hat{V}}$. نعرف التطبيق $\psi:V\to\hat{\hat{V}}$ على النحو $v\psi=T_v$ لكل v في V . يقودنا هذا إلى السؤال: هل ψ تشاكل من V إلى $\hat{\hat{V}}$ ؟ حقا إنه كذلك لأن

$$T_{v+w}(f)=f(v+w)=f(v)+f(w)=T_v(f)+T_w(f)$$
$$=(T_v+T_w)(f)$$

مما يثبت أن: $T_{v+w}=T_v+T_w$ أي أن $(v+w)\psi=v\psi+w\psi$

وبصورة مشابهة نحصل على $(\lambda v)\psi=\lambda(v\psi)$ لكل λ في F. وهكذا نجد أن ψ يعرف تشاكلا من V إلى $\hat{\hat{V}}$ وهذا التعريف لا يعتمد على اختيار أساس ولا على خواص معينة للفضاء V، إنه مثال على إنشاء ثابت.

ونسأل الآن: متى يكون ψ تماثلاً؟ للإجابة على ذلك يجب أن نعرف متى $v\psi=0$ أو بصورة مكافئة متى $T_v=0$. ولكن إذا كان $T_v=0$ فإن $0=T_v(f)=f(v)$ لجميع f في $\hat{V}$. بيد أننا بيّنا بدون برهان أنه في فضاء المتجهات العام إذا أعطينا $v\neq0$ فبإمكاننا إيجاد f في $\hat{V}$ بحيث $f(v)\neq0$. في الحقيقة أننا برهنّا على ذلك في حالة كون V منتهي البعد على F. لذا فلأي فضاء منتهي البعد (وفي الحقيقة لأي فضاء اختياري) يكون ψ تماثلاً. وبالإضافة إلى ذلك يكون ψ تماثلاً على $\hat{\hat{V}}$ عندما يكون V منتهي البعد. ونود أن نشير إلى أن ψ لا يكون غامرا في حالة V غير منتهي البعد على F.

إذا كان V منتهي البعد فوفقاً للنتيجة الثانية من مبرهنة (٤-٣-١) يتساوى بُعْدَا V و $\hat{V}$ وكذلك بُعْدَا $\hat{V}$ و $\hat{\hat{V}}$ ولما كان ψ تماثلا من V إلى $\hat{\hat{V}}$ فإن تساوي البعدين يجعل ψ غامراً. بما سبق نكون قد برهنّا التمهيدية التالية.

تمهيدية (٤-٢-٣)

إذا كان V منتهي البعد، فإن ψ تماثل من V على $\hat{\hat{V}}$.

من الآن فصاعداً سنطابق V و $\hat{\hat{V}}$ واضعين في أذهاننا أن هذا التطابق يتم بواسطة التماثل ψ.

تعريف:

إذا كان W فضاءًا جزئياً من V فإن ***مُفْنى*** *W (annihilator) ونرمز له بالرمز $A(W)$ هو مجموعة جميع العناصر f في $\hat{V}$ بحيث $f(w)=0$ لجميع w في W.*

نترك للقارىء التحقق من أن $A(W)$ هو فضاء جزئي من $\hat{V}$.
من الواضح أنه إذا كان $U \subset W$ فإن $A(U) \supset A(W)$.

ليكن V فضـاء متجهـات منتهي البعد و W فضاءًا جزئيا من V . إذا كان f في $\hat{V}$ و $\bar{f}$ اقتصـار f على W ، أي أن $\bar{f}$ معرّفة على W بواسطة $\bar{f}(w)=f(w)$ لكـل w في W . من الواضح أن $\bar{f}$ في $\hat{W}$ لأن f في $\hat{V}$. لننـظر إلى التـطبيق $T: \hat{V} \to \hat{W}$ المعـرّف بواسطة $fT=\bar{f}$ لكل f في $\hat{V}$. فمن السهولة أن نرى أن: $(f+g)T=fT+gT$ وكذلك $(\lambda f)T=\lambda(fT)$. لذا نجد أن T تشاكل من $\hat{V}$ إلى $\hat{W}$. والآن نسأل: ما هي نواة T ؟

إذا كان f في نواة T فإن اقـتـصـار f على W يجب أن يكـون 0 ، أي أن $f(w)=0$ لكـل w في W . وبـالعكس إذا كان $f(w)=0$ لكـل w في W فإن f يقـع في نواة T . إذن نواة T هي بالضبط $A(W)$.

الآن نزعم أن التـطبيق T يغمر الفضاء $\hat{W}$. إن ما نريد بيانه هو أن أي عنصر h في $\hat{W}$ عبـارة عن اقـتـصـار لعـنصر f في $\hat{V}$ ، أي أن $h=\bar{f}$. وَفْـقـاً لتـمهيدية (٤-٢-٥) إذا كان $w_1,\ldots,w_m$ أسـاسـاً في W فبـإمكـاننا توسيعه إلى أساس في V على الصيغـة $w_1,\ldots,w_m,v_1,\ldots,v_r$ حيث $r+m=\dim V$. ليكن W_1 الفضـاء الجـزئي من V المولّد بواسطة $v_1,\ldots,v_r$ ، فيكون $V=W\oplus W_1$.

إذا كان h في $\hat{W}$ فعـرف f في $\hat{V}$ على النحو: ليكن v في V مكتوبا على الصيغة $v=w+w_1$ حيث w في W و w_1 في W_1 عندئذ $f(v)=h(w)$. من الـسـهـل الـتـحـقـق من أن f في $\hat{V}$ وأن $\bar{f}=h$ مما يجعل $h=fT$ ويكون T تطبيقاً من $\hat{V}$ على $\hat{W}$. باستعـمال مبرهنة (٤-١-١) يكون $\hat{W}$ متماثلاً مع $\hat{V}/A(W)$ لأن $A(W)$ تساوي نواة T . نستنتج من ذلـك أن: $\dim(\hat{W})=\dim(\hat{V}/A(W))$ ليكـن $m=\dim W$ ، $n=\dim V$ و $r=\dim A(W)$. وَفْقـاً لنتيجـة (٢) من مبرهنـة (٤-٣-١) $m=\dim\hat{W}$ و $n=\dim\hat{V}$ ولكن باستعمال تمهيدية (٤-٢-٦) يكون

$$\dim\hat{V}/A(W)=\dim\hat{V}-\dim A(W)=n-r$$

مما يجعل $m=n-r$. وبنقل الحدود نحصل على $r=n-m$ وبذلك نكون قد برهنّا على ما يلي :

مبرهنة (٤-٣-٢)

إذا كان V منتهي البعد و W فضاءً جزئياً من V ، فإن $\hat{W}$ يماثل $\hat{V}/A(W)$ و $\dim A(W)=\dim V-\dim W$.

نتيجة

$$A(A(W)) = W$$

البرهان

أولاً ، من أجل أن يكون للنتيجة معنى لاحظ أن $A(A(W))\subset\hat{\hat{V}}$ فلا بد من مطابقة V مع $\hat{\hat{V}}$. الآن ليكن w في W عندئذ $w\psi=T_w$ حيث $T_w(f)=f(w)$ و $f(w)=0$ لكل f في $A(W)$ مما يجعل $W\subset A(A(W))$. ولكن

$$\dim A(A(W))=\dim\hat{\hat{V}}-\dim A(W)$$

(بتطبيق المبرهنة على فضاء المتجهات $\hat{V}$ وفضائه الجزئي $A(W)$) لذا

$$\dim A(A(W))=\dim\hat{\hat{V}}-\dim A(W)=\dim V-(\dim V-\dim W)=\dim W$$

أي أن W و $A(A(W))$ لهما البعد نفسه. ولكون $W\subset A(A(W))$ نستنتج أن $W=A(A(W))$.

إن للمبرهنة (٤-٣-٢) تطبيق على دراسة نظام المعادلات الخطية المتجانسة. لنعتبر النظام الحاوي على m من المعادلات في n من المجاهيل.

$$a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=0,$$
$$a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=0,$$
$$a_{m1}x_1+a_{m2}x_2+\ldots+a_{mn}x_n=0,$$

حيث a_{ij} في F . ونسأل عن عدد الحلول $(x_1,\ldots,x_n)$ في $F^{(n)}$ المستقلة خطيا لهذا النظام.

في $F^{(n)}$ ليكن U الفضاء الجزئي المولّد من المتجهات $(a_{11},a_{12},\ldots,a_{1n})$ ، $(a_{21},a_{22},\ldots,a_{2n})$ ، . . . ، $(a_{m1},a_{m2},\ldots,a_{mn})$ التي عددها m وافرض أن بعد U يساوي r . في هذه الحالة نقول إن نظام المعادلات هو من **المرتبة** r (rank) .

ليكن $v_1=(1,0,\ldots,0)$ ، $v_2=(0,1,0,\ldots,0)$ ، . . . ، $v_n=(0,0,\ldots,0,1)$ ، الأساس المستعمل للفضاء $F^{(n)}$. وليكن $\hat{v}_1,\hat{v}_2,\ldots,\hat{v}_n$ الأساس الثنوي في $\hat{F}^{(n)}$. إن كل عنصر f في $\hat{F}^{(n)}$ هو على الهيئة

$$f=x_1\hat{v}_1+\ldots+x_n\hat{v}_n$$

حيث x_i في F .

الآن نسأل: متى يكون f في A(U) ؟ في هذه الحالة، لكون $(a_{11},\ldots,a_{1n})$ في U نحصل على

$$\begin{aligned}0&=f(a_{11},a_{12},\ldots,a_{1n})\\&=f(a_{11}v_1+\ldots+a_{1n}v_n)\\&=(x_1\hat{v}_1+x_2\hat{v}_2+\ldots+x_n\hat{v}_n)(a_{11}v_1+\ldots+a_{1n}v_n)\\&=x_1a_{11}+x_2a_{12}+\ldots+x_na_{1n}\end{aligned}$$

لأن $\hat{v}_i(v_j)=0$ إذا كان $i\neq j$ و $\hat{v}_i(v_i)=1$.

وبصورة مشابهة تتحقق باقي معادلات النظام. وبالعكس كل حل $(x_1,\ldots,x_n)$ لنظام المعادلات المتجانسة ينتج عنه عنصر $x_1\hat{v}_1+\ldots+x_n\hat{v}_n$ في A(U) .

مما تقدم نرى أن عدد الحلول المستقلة خطياً لنظام المعادلات يساوي بعد A(U) والذي يساوي n−r وَفْقاً لمبرهنة (٤-٣-٢) وبذلك نكون قد برهنا على ما يلي:

مبرهنة (٤-٣-٣)

إذا كان نظام المعادلات الخطية المتجانسة

$$a_{11}x_1+\ldots+a_{1n}x_n=0$$

$$a_{21}x_1+\ldots+a_{2n}x_n=0$$
$$a_{m1}x_1+\ldots+a_{mn}x_n=0$$

حيث a_{ij} في F من المرتبة r ، فيوجد $n-r$ من الحلول المستقلة خطيا في $F^{(n)}$.

نتيجة

إذا كان $n>m$ ، أي إذا كان عدد المجاهيل يزيد على عدد المعادلات فيوجد حل $(x_1,\ldots,x_n)$ لا يساوي الصفر في $F^{(n)}$.

البرهان

لأن U مولَّد بواسطة m من المتجهات و $m<n$ ، فإن $r=\dim U\leq m<n$.
بتطبيق المبرهنة (٤-٣-٣) نحصل على النتيجة.

مسائل

١ - برهن على أن $A(W)$ فضاء جزئي من $\hat{V}$

٢ - إذا كانت S مجموعة جزئية من V و $A(S)$ مجموعة كل العناصر f في $\hat{V}$ بحيث $f(s)=0$ لجميع العناصر s في S . فبرهن على أن $A(S)=A(L(S))$ حيث $L(S)$ هو الفضاء الجزئي المتولد من S .

٣ - إذا كان T,S في Hom (V,W) و $v_iS=v_iT$ لجميع العناصر v_i في أساس من V . فبرهن على أن $S=T$

٤ - أكمل برهان أن Hom (V,W) هو فضاء متجهات معطياً جميع التفاصيل.

٥ - إذا كان ψ يرمز للتطبيق المستعمل في الشرح من V إلى $\hat{\hat{V}}$. فأعط برهاناً كاملاً على أن ψ هو تشاكل فضاء متجهات من V إلى $\hat{\hat{V}}$.

٦ - إذا كان V منتهي البعد و $v_1\neq v_2$ في V . فبرهن على أنه يوجد عنصر f في $\hat{V}$ بحيث $f(v_1)\neq f(v_2)$.

٧ - إذا كان W_2,W_1 فضاءين جزئيين من V المنتهي البعد. فصف $A(W_1+W_2)$ بدلالة $A(W_2), A(W_1)$.

٨ - إذا كان V منتهي البعد و W_2, W_1 فضاءين جزئيين من V . فصف $A(W_1 \cap W_2)$ بدلالة $A(W_2), A(W_1)$.

٩ - إذا كان F حقل الأعداد الحقيقية . فأوجد $A(W)$ حيث

(أ) W مولد بواسطة $(1,2,3)$ و $(0,4,-1)$.

(ب) W مولد بواسطة $(0,0,1,-1)$ ، $(2,1,1,0)$ و $(2,1,1-1)$.

١٠ - أوجد مراتب نظام المعادلات الخطية المتجانسة التالية على F ، حقل الأعداد الحقيقية ثم أوجد جميع الحلول .

(أ)
$$x_1+2x_2-3x_3+4x_4=0,$$
$$x_1+3x_2-x_3=0$$
$$6x_2+x_3+2x_4=0.$$

(ب)
$$x_1+3x_2+2x_3=0$$
$$x_1+4x_2+x_3=0.$$

(جـ)
$$x_1+x_2+x_3+x_4+x_5=0$$
$$x_1+2x_2=0$$
$$4x_1+7x_2+x_3+x_4+x_5=0$$
$$x_2-x_3-x_4-x_5=0$$

١١ - إذا كان g, f في $\hat{V}$ بحيث $f(v)=0$ يقتضي أن $g(v)=0$. فبرهن على أن $g=\lambda f$ حيث λ في F .

(٤ - ٤) فضاءات الضرب الداخلي

في دراستنا لفضاء المتجهات وجدنا أن الطبيعة الخاصة للحقل F باستثناء كونه حقلا لم تلعب دورا يذكر . في هذا البند سنقصر دراستنا لفضاءات المتجهات على حقلي الأعداد الحقيقية والمركبة بدلا من أي حقل اختياري وسنطلق على الفضاء V اسم **فضاء متجهات حقيقي** (real vector space) في حالة حقل الأعداد الحقيقية **وفضاء متجهات مركب** (complex vector space) في حالة حقل الأعداد المركبة .

إن لدينا بعض الخبرة في التعامل مع فضاءات المتجهات الحقيقية ـ في الحقيقة أن الهنـدسة التحليلية والتحليل المتجهي يتعاملان مع مثل هذه الفضاءات. والآن نسأل: ما هي المفاهيم التي يمكن نقلها إلى صياغة أكثر تجريدا؟

أولا: كان لدينا في تلك المواضيع مفهوم للطول.

ثانيا: كان لدينا فكرة التعامد، أو بصورة عامة، فكرة الزاوية.

هذه أصبحت حالات خاصة من مفهوم **الضرب النقطي** (dot product) (ويطلق عليه عادة اسم **الضرب القياسي** (scalar product) أو **الداخلي** (inner product)).

الآن لنستذكر بعض خواص الضرب النقطي فيما يتعلق بالحالة الخاصة للمتجهات الحقيقية الثلاثية البعد.

إذا كان لدينا المتجهان $v=(x_1,x_2,x_3)$ و $w=(y_1,y_2,y_3)$ حيث x_i و y_i أعداد حقيقية. فإن الضرب النقطي للمتجهين v و w ونرمز له بالرمز $v.w$ يعرف كما يلي $x_1y_1+x_2y_2+x_3y_3$.

لاحظ أن طول v يساوي $\sqrt{v.v}$ والزاوية θ بين v و w تُعطى بالصيغة

$$\cos\theta=\frac{v.w}{\sqrt{v.v}\,\sqrt{w.w}}$$

إن السؤال الذي يطرح نفسه هو: ما هي الخواص الشكلية لهذا الضرب؟

نسرد بعضا منها:

١ ـ $v.v\geqslant 0$ و $v.v=0$ إذا وفقط إذا كان $v=0$

٢ ـ $v.w = w.v$

٣ ـ $u.(\alpha v+\beta w) = \alpha(u.v) + \beta(u.w)$

لأي متجهات u,v,w وعددين حقيقيين α و β.

كل ما قيل يمكن تعميمه إلى فضاء المتجهات المركب. ولكن للحصول على تعاريف هندسية معقولة يجب إجراء بعض التعديلات. فإذا عرَّفنا $v.w = x_1y_1 + x_2y_2 + x_3y_3$

للمتجهين $v=(x_1,x_2,x_3)$ و $w=(y_1,y_2,y_3)$ حيث x_i و y_i أعداد مركبة . فإنه من الممكن أن يكون $v.v=0$ و $v\neq0$. يمكننا توضيح ذلك بالمتجه $v=(1,i,0)$ ، في الواقع أن $v.v$ قد لا يكون عددا حقيقيا . إذا أردنا، كما هي الحالة في فضاءات المتجهات الحقيقية، أن يكون $v.v$ ممثلا بطريقة ما لطول v ، فمن الأجدر أن يكون هذا الطول عددا حقيقيا وأن يكون للمتجه غير الصفري طول لا يساوي الصفر.

إن من الممكن تحقيق ما أشرنا إليه بتغيير تعريف الضرب النقطي بعض الشيء . فإذا كان $\bar{\alpha}$ يرمز إلى مرافق العدد المركب α ، فإننا نعرف الضرب النقطي للمتجهين v و w المذكورين أعلاه على أنه :

$$v.w = x_1\bar{y}_1 + x_2\bar{y}_2 + x_3\bar{y}_3$$

في حالة المتجهات الحقيقية يتفق التعريف الجديد هذا مع التعريف القديم وفي حالة المتجهات المركبة الاختيارية $v\neq0$ لا يكون $v.v$ حقيقيا فحسب ولكنه في الحقيقة عدد موجب. لذا فباستطاعتنا تعريف طول غير سالب للمتجهات المركبة. ولكننا نخسر بعض الخصائص مثل $v.w=w.v$ التي لا تكون صحيحة . وفي الواقع يكون لدينا في هذه الحالة العلاقة $v.w=\overline{w.v}$.

الآن نسرد بعض خصائص هذا الضرب النقطي

١ - $v.w = \overline{w.v}$

٢ - $v.v\geq0$ و $v.v=0$ إذا وفقط إذا كان $v=0$

٣ - $(\alpha u+\beta v).w = \alpha(u.w) + \beta(v.w)$

٤ - $u.(\alpha v+\beta w) =\bar{\alpha}(u.v) + \bar{\beta}(u.w)$

لكل الأعداد المركبة α و β والمتجهات المركبة u ، v و w.

نؤكد ثانية أن F يرمز إلى حقل الأعداد الحقيقية أو المركبة في كل ما سيأتي من هذا البند.

تعريف

يقال إن فضاء المتجهات V على F ***فضاء ضرب داخلي*** *(inner product space) إذا كان معرفا لكل متجهين u و v في V عنصر (u,v) في F بحيث:*

١ ـ $(u,v) = \overline{(v,u)}$

٢ ـ $(u,u) \geqslant 0$ و $(u,u)=0$ إذا وفقط إذا كان $u=0$

٣ ـ $(\alpha u+\beta v,w) = \alpha(u,w) + \beta(v,w)$

لكل u ، v و w في V و α ، β في F.

هنا بعض الملاحظات الواجب ذكرها حول الخواص ١ ، ٢ ، ٣ أعلاه.

أولها: أن الدالة التي تحقق هذه الخواص تسمى ضربا داخليا.

وثانيها: أنه إذا كان F حقل الأعداد المركبة فإن الخاصة ١ تقتضي أن يكون (u,u) عددا حقيقيا مما يجعل للخاصة ٢ معنى.

أما الملاحظة الثالثة: فهي أنه باستعمال ١ و ٣ نجد أن:

$$(u,\alpha v+\beta w) = \overline{(\alpha v+\beta w,u)} = \overline{\alpha(v,u) + \beta(w,u)} =$$
$$= \bar{\alpha}\overline{(v,u)} + \bar{\beta}\overline{(w,u)} = \bar{\alpha}(u,v) + \bar{\beta}(u,w).$$

الآن نتوقف لننظر إلى بعض الأمثلة على فضاءات الضرب الداخلي.

مثال (٤-٤-١)

في $F^{(n)}$ عرف للمتجهين $u=(\alpha_1,\ldots,\alpha_n)$ و $v=(\beta_1,\ldots,\beta_n)$ المقدار

$$(u,v)= \alpha_1\bar{\beta}_1+\alpha_2\bar{\beta}_2+\ldots+\alpha_n\bar{\beta}_n$$

إن هذا يعرف ضربا داخليا على $F^{(n)}$.

مثال (٤-٤-٢)

في $F^{(2)}$ عرف للمتجهين $u=(\alpha_1,\alpha_2)$ و $v=(\beta_1,\beta_2)$ المقدار

$$(u,v)=2\alpha_1\bar{\beta}_1 +\alpha_1\bar{\beta}_2+\alpha_2\bar{\beta}_1+\alpha_2\bar{\beta}_2.$$

من السهل التحقق من أن هذا يعرف ضربا داخليا على $F^{(2)}$.

مـــثـــال (٤-٤-٣)

لتكن V مجموعة جميع الدوال المتصلة ذات القيمة المركبة المعرفة على فترة الوحدة المغلقة [0,1] .

إذا كانت f(t) و g(t) في V فعرف :

$$(f(t), g(t)) = \int_0^1 f(t)g(t)dt$$

نترك للقارىء التحقق من أن هذا يعرف ضربا داخليا على V.

فيما سيأتي في هذا البند V يعني فضاء ضرب داخلي .

تعريف

*إذا كان v في V فإن **طول** (length) v (أو **معيار** (norm) v) مكتوبا $||v||$ يعرف على أنه :*

$$||v|| = \sqrt{(v,v)}$$

تمهيدية (٤-٤-١)

إذا كان u ، v في V و α ، β في F فإن

$$(\alpha u+\beta v,\alpha u+\beta v)=\alpha\bar{\alpha}(u,u)+\alpha\bar{\beta}(u,v)+\bar{\alpha}\beta(v,u)+\beta\bar{\beta}(v,v)$$

البرهان

وفقا للخاصة (٣) في تعريف فضاء الضرب الداخلي يكون :

$$(\alpha u+\beta v,\alpha u+\beta v)=\alpha(u,\alpha u+\beta v)+\beta(v,\alpha u+\beta v)$$

ولكن

$$(u,\alpha u+\beta v)=\bar{\alpha}(u,u)+\bar{\beta}(u,v)$$

و

$$(v,\alpha u+\beta v)=\bar{\alpha}(v,u)+\bar{\beta}(v,v)$$

بتعويض هذه في العبارة $(\alpha u+\beta v,\alpha u+\beta v)$ أعلاه نحصل على النتيجة المطلوبة.

نتيجـــة

$$\|\alpha u\|=|\alpha|\,\|u\|$$

البرهان

$\|\alpha u\|^2=(\alpha u,\alpha u)=\alpha\bar{\alpha}(u,u)$ وفقا لتمهيدية (٤-٤-١) (حيث $v=0$).

ولما كان $\alpha\bar{\alpha}=|\alpha|^2$ ، $(u,u)=\|u\|^2$ فبأخذ الجذر التربيعي للطرفين في أعلاه نحصل على:

$$\|\alpha u\|=|\alpha|\,\|u\|$$

الآن نحيد عن سير دراستنا بعض الشيء لنبرهن على نتيجة مألوفة وأساسية حول المعادلات الحقيقية من الدرجة الثانية.

تمهيدية (٤-٤-٢)

إذا كانت a ، b و c أعدادا حقيقية بحيث $a>0$ و $a\lambda^2+b\lambda+c\geqslant 0$ لكل الأعداد الحقيقية λ ، فإن $b^2\leqslant ac$.

البرهان

بإكمال المربع نحصل على

$$a\lambda^2+2b\lambda+c=\frac{1}{a}(a\lambda+b)^2+\left(c-\frac{b^2}{a}\right)$$

ولما كان الجانب الأيسر أكبر أو يساوي صفرا لجميع قيم λ الحقيقية، فإن هذا يجب أن يكون صحيحا عندما $\lambda=-b/a$ على وجه الخصوص. ومن ذلك نحصل على أن $c-(b^2/a)\geqslant 0$ ، ولكون $a>0$ نجد أن $b^2\leqslant ac$.

الآن نقدم متباينة ذات أهمية كبرى تدعى متباينة شوارتز.

مبرهنة (٤-٤-١)

إذا كان u و v في V فإن $|(u,v)|\leq||u||\,||v||$

البرهان

إذا كان $u=0$ فإن كلا من $(u,v)=0$ و $||u||\,||v||=0$ مما يجعل المتباينة صحيحة في هذه الحالة.

الآن نفرض أن (u,v) عدد حقيقي و $u\neq0$. إذا كان λ أي عدد حقيقي فوفقا لتمهيدية (٤-٤-١) يكون

$$0\leq(\lambda u+v,\lambda u+v)=\lambda^2(u,u)+2\lambda(u,v)+(v,v)$$

ليكن $a=(u,u)$ و $b=(u,v)$ و $c=(v,v)$ عندئذ جميع فرضيات تمهيدية **(٤-٤-٢)** متحققة مما يجعل $b^2\leq ac$. أي أن $(u,v)^2\leq(u,u)(v,v)$ ومن هذا نستنتج أن: $|(u,v)|\leq||u||\,||v||$

إذا كان $\alpha=(u,v)$ غير حقيقي فمن المؤكد أنه لا يساوي صفرا أي أن للمتجه u/α معنى. الآن:

$$(\frac{u}{\alpha},v)=\frac{1}{\alpha}(u,v)=\frac{1}{(u,v)}(u,v)=1$$

وهو حقا عدد حقيقي.

باستخدام حالة متباينة شوارتز التي شرحناها في الفقرة أعلاه نحصل على

$$1=|(\frac{u}{\alpha},v)|\geq||\frac{u}{\alpha}||\,||v||$$

ولما كان

$$||\frac{u}{\alpha}||=\frac{1}{|\alpha|}||u||$$

فإننا نستنتج أن

$$1\leq\frac{||u||\,||v||}{|\alpha|}$$

أي أن

$$|\alpha| \leqslant \|u\|\,\|v\|$$

بالتعويض عن قيمة α بالمقدار (u,v) نحصل على : $|(u,v)| \leqslant \|u\|\,\|v\|$

وهي النتيجة المطلوبة.

بعض الحالات الخاصة من متباينة شوارتز يكون لها أهمية كبرى بحد ذاتها ونشير هنا إلى حالتين منها :

١ - إذا كان $V=F^{(n)}$ و $(u,v)=\alpha_1\bar{\beta}_1+..+\alpha_n\bar{\beta}_n$ حيث $u=(\alpha_1,\ldots,\alpha_n)$ و $v=(\beta_1,\ldots,\beta_n)$ فإن مبرهنة ٤-٤-١ تقتضي أن :

$$|\alpha_1\bar{\beta}_1+\ldots+\alpha_n\bar{\beta}_n|^2 \leqslant (|\alpha_1|^2+\ldots+|\alpha_n|^2)(|\beta_1|^2+\ldots+|\beta_n|^2)$$

٢ - إذا كانت V مجموعة جميع الدوال المتصلة وذات القيمة المركبة المعرفة على $[0,1]$ حيث إن الضرب الداخلي معرف بواسطة :

$$(f(t),g(t))=\int_0^1 f(t)\overline{g(t)}dt$$

فإن مبرهنة ٤-٤-١ تقتضي أن :

$$\left|\int_0^1 f(t)g(t)dt\right|^2 \leqslant \int_0^1 |f(t)|^2dt\int_0^1 |g(t)|^2dt$$

إن مفهوم التعامد مفيد جدا وله أهميته في الهندسة، نقدم هنا ما يقابله في الحالة العامة لفضاءات الضرب الداخلي.

تعريف

*إذا كان u و v في V فيقال إن u **عمودي** (orthogonal) على v إذا كان $(u,v)=0$.*

لاحظ أنه إذا كان u عموديا على v فإن v عمودي على u لأن $(v,u)=(\overline{u,v})=\bar{0}=0$

تعريف

إذا كان W فضاء جزئيا من V ***فإن المتمم العمودي (orthogonal complement)*** *على W والذي نرمز له بالرمز $W^{\perp}$ يعرف على أنه مجموعة جميع العناصر x في V بحيث $(x,w)=0$ لجميع العناصر w في W.*

تمهيدية (٤-٤-٣)

$W^{\perp}$ يكون فضاء جزئيا من V.

البرهان

إذا كان a و b في $W^{\perp}$ فإنه لجميع العناصر α و β في F وكل عنصر w في W يكون:

$$(\alpha a+\beta b,w)=\alpha(a,w)+\beta(b,w)=0$$

لأن a و b في $W^{\perp}$

لاحظ أن $W\cap W^{\perp}=(0)$ لأنه إذا كان w في $W\cap W^{\perp}$ فيجب أن يكون عموديا على نفسه أي أن $(w,w)=0$ مما يجعل $w=0$ وذلك بالرجوع إلى الخواص المعرفة لفضاء الضرب الداخلي.

إن من أهدافنا هو أن نبين أن $V=W+W^{\perp}$ وعند انتهائنا من ذلك سيصبح للملاحظة المذكورة أعلاه أهمية لأنها ستقتضي أن يكون V مجموعًا مباشرا للفضاءين الجزئيين W و $W^{\perp}$.

تعريف

يقال عن مجموعة من المتجهات $\{v_i\}$ في V ***إنها مجموعة متعامدة معايرة*** *(orthonormal set) إذا كان:*

١ - *طول كل v_i يساوي 1 (بمعنى أن $(v_i,v_i)=1$)*

٢ - *$(v_i,v_j)=0$ لكل $i\neq j$*

تمهيدية (٤-٤-٤)

إذا كانت $\{v_i\}$ مجموعة متعامدة معايرة فإن المتجهات في $\{v_i\}$ مستقلة خطيا.

إذا كان $w=\alpha_1 v_1+\ldots+\alpha_n v_n$ فإن $\alpha_i=(w,v_i)$ لكل $i=1,2,\ldots,n$.

البرهان

افرض أن:

$$\alpha_1 v_1+\ldots+\alpha_n v_n=0$$

فنحصل على:

$$0=(\alpha_1 v_1+\ \ldots+\alpha_n v_n,\ v_i)=\alpha_1(v_1,v_i)+\ldots+\alpha_n(v_n,v_i)$$

ولكن $(v_j,v_i)=0$ لكل $j\neq i$ و $(v_i,v_i)=1$ مما يجعل المعادلة أعلاه تؤول إلى $\alpha_i=0$ وهكذا نجد أن المتجهات v_i مستقلة خطيا.

إذا كان $w=\alpha_1 v_1+\ldots+\alpha_n v_n$ فبإجراء الحسابات كما في أعلاه نحصل على $(w,v_i)=\alpha_i$.

التمهيدية التالية تشبه تمهيدية (٤-٤-٤) في طبيعتها وبرهانها.

تمهيدية (٤-٤-٥)

إذا كانت $\{v_i,\ldots,v_n\}$ مجموعة متعامدة معايرة في V و w في V، فإن

$$u=w-(w,v_1)\,v_1-(w,v_2)v_2-\ldots-(w,v_i)v_i-\ldots-(w,v_n)v_n$$

يكون عمودي على كل من $v_1,v_2,\ldots,v_n$

البرهان

بحساب (u,v_i) لكل $i\leqslant n$ وذلك باستعمال خاصة التعامد المعايرة للمتجهات $v_1,\ldots,v_n$ نحصل على النتيجة.

إن البناء الذي سيوجد في إثبات المبرهنة القادمة يظهر بكثرة في العديد من فروع الرياضيات. إن الطريقة المستعملة تعتبر أساسية وتسمى **طريقة جرام ـ شمدت في التعامد** (Gram-Schmidt orthogonalization process).

بالرغم من أننا سنعمل داخل فضاء ضرب داخلي منتهي البعد، فإن طريقة جرام شمدت تصلح للعمل في حالة الفضاءات غير المنتهية البعد.

مبرهنة (٤-٤-٢)

إذا كان V فضاء ضرب داخلي منتهي البعد، فإن V يحوي مجموعة متعامدة معايرة كأساس له.

البرهان

ليكن بعد V على F يساوي n و $v_1,\ldots,v_n$ أساسا للفضاء V. من هذا الأساس سوف ننشىء مجموعة متعامدة معايرة تحوي n من المتجهات ووفقا لتمهيدية (٤-٤-٤). هذه المتجهات مستقلة خطيا مما يجعلها تكون أساسا في V.

الآن نبدأ البناء. إننا نبحث عن n من المتجهات $w_1,\ldots,w_n$ طول كل منها 1 ولكل $i\neq j$ $(w_i,w_j)=0$. في الواقع إننا سنحصل في النهاية على هذه المتجهات في الشكل التالي:

المتجه w_1 سيكون مضاعفا من v_1 ، w_2 سيكون في التوليد الخطي من w_1 ، v_2 و w_3 في التوليد الخطي من w_1 ، w_2 و v_3. وبصورة عامة سيكون w_i في التوليد الخطي من $w_1,w_2,\ldots,w_{i-1},v_i$.

ليكن

$$w_1=\frac{v_1}{||v_1||}$$

عندئذ

$$(w_1,w_1)=(\frac{v_1}{||v_1||},\frac{v_1}{||v_1||})=\frac{1}{||v_1||^2}(v_1,v_1)=1$$

مما يؤدي إلى أن

$$||w_1||=1$$

الآن نسأل: أية قيمة للعدد α تجعل αw_1+v_2 عموديا على w_1 ؟

كل ما نحتاج إليه هو $(\alpha w_1+v_2,w_1)=0$ أي أن: $\alpha(w_1,w_1)+(v_2,w_1)=0$

وبما أن $(w_1,w_1)=1$ يكون $\alpha=-(v_2,w_1)$ وهذا العدد يؤدي الغرض المطلوب. ليكن: $u_1=-(v_2,w_1)w_1+v_2$ ، فيكون u_2 عموديا على w_1 ولما كـان v_1 و v_2 مستقلين خطيا فإنه يجب أن يكون w_1 و v_2 مستقلين خطيا مما يؤدي إلى أن $u_2\neq0$.

ليكن $w_2=\frac{u_2}{||u_2||}$ فنحصل على المجموعة المتعامدة المعايرة $\{w_1,w_2\}$

نستمر على هذا المنوال فنجعل $u_3=-(v_3,w_1)w_1-(v_3,w_2)w_2+v_3$. إن من السهل التحقق من أن $(u_3,w_1)=(u_3,w_2)=0$. ولما كانت w_2,w_1 و v_3 مستقلة خطيا (لأن w_1 ، w_2 يقعان في التوليد الخطي للمتجهين v_2,v_1) فإننا نحصل على $u_3\neq0$.

ليكن $w_3=\frac{u_3}{||u_3||}$ فتكون المجموعة $\{w_1,w_2,w_3\}$ متعامدة معايرة.

والآن يبـدو الأمـر أمـامنا واضحا. نفرض أننا أنشأنا $w_1,w_2,\ldots,w_i$ في التوليد الخطي للمتجهات $v_1,\ldots,v_i$ بحيث أنها تكون مجموعة متعامدة معايرة. كيف ننشىء المتجه التالي w_{i+1} ؟

نجعل

$$u_{i+1}=-(v_{i+1},w_1)w_1-(v_{i+1},w_2)w_2-\ldots-(v_{i+1},w_i)w_i+v_{i+1}$$

ونترك للقارىء التحقق من أن $u_{i+1}\neq0$ وأنه عمودي على $w_1,\ldots,w_i$ ليكن $w_{i+1}=\frac{u_{i+1}}{||u_{i+1}||}$

بهذه الطريقة إذا أعطينا r من المتجهات المستقلة خطيا في V فيمكننا أن ننشىء مجموعة متعامدة معايرة تحوي r من العناصر. وعلى وجه الخصوص عندما $\dim V=n$

فمن أي أساس في V يمكن أن ننشىء مجموعة متعامدة معايرة تحوي n من العناصر. هذا يعطينا الأساس المطلوب للفضاء V.

الآن نوضح طريقة البناء المستعملة في البرهان في الحالة التالية: ليكن F حقل الأعداد الحقيقية و V مجموعة كثيرات الحدود في المتغير x على الحقل F من الدرجة 2 أو أقل. نعرف في V ضربا داخليا على النحو التالي:

إذا كان $p(x)$ و $q(x)$ في V فإن:

$$(p(x), q(x) = \int_{-1}^{1} p(x)q(x)dx$$

لنبدأ بالأساس $v_1=1$ ، $v_2=x$ و $v_3=x^2$ في V. باتباعنا لطريقة البناء أعلاه نجعل

$$w_1=\frac{v_1}{||v_1||}=\frac{1}{\sqrt{\int_{-1}^{1}1dx}}=\frac{1}{\sqrt{2}},$$

$$u_2=-(v_2,w_1)w_1+v_2$$

وبعد إجراء الحسابات نحصل على $u_2=x$ ومن ثم:

$$w_2=\frac{u_2}{\|u_2\|}=\frac{x}{\sqrt{\int_{-1}^{1}(x^2dx)}}=\frac{\sqrt{3}}{\sqrt{2}}x$$

وأخيرا:

$$u_3=-(v_3,w_1)w_1-(v_3,w_2)w_2+v_3=-\frac{1}{3}+x^2$$

فيكون

$$w_3=\frac{u_3}{\|u_3\|}=\frac{-\frac{1}{3}+x^2}{\sqrt{\int_{-1}^{1}\left(-\frac{1}{3}+x^2\right)^2dx}}=\frac{\sqrt{10}}{4}(-1+3x^2)$$

سبق أن ذكرنا أن المبرهنة التالية هي أحد أهدافنا. يمكننا الآن إثباتها.

مبرهنة (٤-٤-٣)

إذا كان V فضاء ضرب داخلي منتهي البعد و W فضاء جزئيا من V ، فإن $V=W+W^{\perp}$. وعلى وجه التحديد V هو الجمع المباشر للفضاءين W و $W^{\perp}$

البرهان

بسبب الطبيعة الهندسية للنتيجة ولكونها أساسية فسوف نقدم برهانين لها. **البرهان الأول** سيستعمل مبرهنة (٤-٤-٢) وبعض التمهديات التي سبقتها، أما **البرهان الثاني** فسيكون ذا دوافع هندسية.

البرهان الأول

يمكن اعتبار W فضاء ضرب داخلي ذلك لأنه فضاء جزئي من فضاء الضرب الداخلي V (إن الضرب الداخلي على W هو اقتصار الضرب في V على W) . لذا يمكننا إيجاد مجموعة متعامدة معايرة $w_1,\dots,w_r$ في W تكوّن أساسا له.
الآن إذا كان v في V فوفقا لتمهيدية (٤-٤-٥) يكون $v_0=v-(v,w_1)w_1-(v,w_2)w_2-\dots-(v,w_r)w_r$ عموديا على كل من $w_1,\dots,w_r$ مما يجعله عموديا على W. وهكذا نجد أن v_0 في $W^{\perp}$ ، ولكن $v=v_0+((v,w_1)w_1+\dots+(v,w_r)w_r)$ مما يجعل v في $W+W^{\perp}$ إذن $V=W+W^{\perp}$. ولما كان $W\cap W^{\perp}=(0)$ يكون هذا الجمع مباشرا.

البرهان الثاني

في هذا البرهان سنفرض أن F هو حقل الأعداد الحقيقية. إن البرهان يبقى صحيحا في حالة حقل الأعداد المركبة بيد أنه يتطلب بعض التفاصيل التي قد تؤثر على وضوح الأفكار الأساسية المستعملة.

ليكن v في V وافرض أنه بإمكاننا إيجاد متجه w_0 في W بحيث $\|v-w_0\|\leq\|v-w\|$ لكل w في W فعندئذ نزعم أن $(v-w_0,w)=0$ لجميع w في W أي أن $v-w_0$ في $W^{\perp}$.
إذا كان w في W فإن $w+w_0$ في W وكنتيجة لذلك يكون:

$$(v-w_0,v-w_0)\leqslant(v-(w_0+w),v-(w_0+w))$$

ولكن الجانب الأيمن هو $(w,w)+(v-w_0,v-w_0)-2(v-w_0,w)$ مما يؤدي إلى $2(v-w_0,w)\leqslant(w,w)$ لكل w في W. إذا كان m أي عدد صحيح موجب فلكون w/m في W نحصل على:

$$\frac{2}{m}(v-w_o,w)=2(v-w_0,\frac{w}{m})\leqslant(\frac{w}{m},\frac{w}{m})=\frac{1}{m^2}(w,w)$$

مما يجعل $2(v-w_0,w)\leqslant\frac{1}{m}(w,w)$ لأي عدد صحيح موجب m. ولكن $\frac{1}{m}(w,w)\to 0$ عندما $m\to\infty$ فيكون $2(v-w_0,w)\leqslant 0$. وبصورة مشابهة، $-w$ في W فيكون:

$$0\leqslant-2(v-w_0,w)=2(v-w_0,-w)\leqslant 0$$

وينتج عن ذلك أن:

$(v-w_0,w)=0$ لكل w في W وهكذا نجد أن $v-w_0$ في $W^\perp$ وبالتالي v في $w_0+W^\perp\subset W+W^\perp$.

كي ننهي البرهان الثاني يجب أن نثبت وجود w_0 في W بحيث $||v-w_0||\leqslant||v-w||$ لكل w في W . سنبين بصورة غير تفصيلية طريقتين لاثبات وجود عنصر مثل w_0.

ليكن $u_1,\ldots,u_k$ أساساً في W لذا يكون أي عنصر w في W على الصيغة $w=\lambda_1u_1+\ldots+\lambda_ku_k$. ليكن $\beta_{ij}=(u_i,u_j)$ و $\gamma_i=(v,u_i)$ لعنصر ما v في V. لذا

$$(v-w,v-w)=(v-\lambda_1u_1-\ldots-\lambda_ku_k,v-\lambda_1u_1-\ldots-\lambda_kw_k)$$
$$=(v,v)-\Sigma\lambda_i\lambda_j\beta_{ij}-2\Sigma\lambda_i\gamma_i$$

إن هذه **الدالة التربيعية** (quadratic function) في λ_s تكون ذات **قيم غير سالبة** (non-negative) فباستعمال حساب التفاضل نجد أن لهذه الدالة قيمة صغرى. نرمز لقيم λ_s، حيث $1\leqslant s\leqslant k$ ، التي تعطينا هذه القيمة الصغرى بالرموز:

$\lambda_1^{(0)},\lambda_2^{(0)},\ldots,\lambda_k^{(0)}$ فيكون $w_0=\lambda_1^{(0)}u_1+\ldots+\lambda_k^{(0)}u_k$ وهو المتجه المطلوب في W.

هناك طريقة أخرى للحصول على مثل هذا العنصر w الذي يعطي قيمة صغرى. عرف في V **المقاس** (metric) ζ بواسطة $\zeta(x,y)=||x-y||$. يمكن التأكد من أن

ع يحقق صفات المقاس على V مما يجعل V **فضاءً مقاسيا** (metric space).

لتكن $S=\{w\in W \mid \|v-w\|\leqslant\|v\|\}$

إن هذه المجموعة متراصة في الفضاء المقاسي V (برهن على ذلك) ولذا يكون للدالة المتصلة $f(w)=\|v-w\|$ والمعرفة لكل w في S قيمة صغرى في نقطة ما w_0 في S . نترك للقارىء التأكد من أن w_0 هو المتجه المطلوب الذي يحقق $\|v-w\|\leqslant\|v-w_0\|$ لكل w في W .

نتيجة

إذا كان V فضاء ضرب داخلي منتهي البعد و W فضاءً جزئيا من V فإن $(W^\perp)^\perp=W$

البرهان

إذا كان w في W فإنه لأي u في $W^\perp$ يكون $(w,u)=0$ مما يجعل $W\subset(W^\perp)^\perp$.

الآن لاحظ أن $V=W+W^\perp$ و $V=W^\perp+(W^\perp)^\perp$ ، ولما كان حاصلا الجمع مباشرين نحصل على $\dim(W)=\dim((W^\perp)^\perp)$. وحيث إن $W\subset(W^\perp)^\perp$ وأن لهذين الفضاءين الجزئيين نفس البعد يكون $W=(W^\perp)^\perp$.

مسائل

في جميع المسائل التالية يكون V فضاء ضرب داخلي على F.

١ ـ إذا كان F حقل الأعداد الحقيقية و $V=F^{(3)}$ فبين أن متباينة شوارتز تقتضي أن جيب تمام الزاوية له قيمة مطلقة تساوي على الأكثر 1 .

٢ ـ إذا كان F حقل الأعداد الحقيقية فأوجد جميع العديدات (a,b,c,d) من رتبة 4 بحيث إنه إذا كان $u=(\alpha_1,\alpha_2)$ و $v=(\beta_1,\beta_2)$ في $F^{(2)}$ فإن :

$$(u,v)=a\alpha_1\beta_1+b\alpha_2\beta_2+c\alpha_1\beta_2+d\alpha_2\beta_1$$

يعرف ضربا داخليا على $F^{(2)}$

٣ - في V عرف المسافة (distance) $\zeta(u,v)$ من u إلى v بواسطة العلاقة $\zeta(u,v)=\|u-v\|$
برهن على أن

(ا) $\zeta(u,v)\geqslant 0$ و $\zeta(u,v)=0$ إذا وفقط إذا كان $u=v$

(ب) $\zeta(u,v)=\zeta(v,u)$

(جـ) $\zeta(u,v)\leqslant\zeta(u,w)+\zeta(w,v)$ (المتباينة المثلثية triangle inequality)

٤ - إذا كانت $\{w_1,\ldots,w_m\}$ مجموعة متعامدة معايرة في V. فبرهن على أن
$\sum_{i=1}^{m}|(w_i,v)|^2\leqslant\|v\|^2$ لأي v في V.

(تسمى هذه المتباينة بمتباينة بَسِلْ Bessel inequality)

٥ - إذا كان V منتهي البعد و $\{w_1,\ldots,w_m\}$ مجموعة متعامدة معايرة في V بحيث :
$\sum_{i=1}^{m}|(w_i,v)|^2=\|v\|^2$ لأي v في V فبرهن على أنه يجب أن تكون $\{w_1,\ldots,w_m\}$ أساسا للفضاء V.

٦ - إذا كان $\dim V=n$ و $\{w_1,\ldots,w_m\}$ مجموعة متعامدة معايرة في V. فبرهن على أنه توجد متجهات $w_{m+1},\ldots,w_n$ بحيث تكون $\{w_1,\ldots,w_m,w_{m+1},\ldots,w_n\}$ مجموعة متعامدة معايرة (وأساس للفضاء V).

٧ - استعمل النتيجة في مسألة ٦ لتقديم برهان آخر للمبرهنة (٤-٤-٣).

٨ - في V برهن على قانون متوازي الأضلاع :

$$\|u+v\|^2+\|u-v\|^2=2(\|u\|^2+\|v\|^2)$$

اشرح ماذا يعني هذا هندسيا في الحالة الخاصة $V=F^{(3)}$ حيث F حقل الأعداد الحقيقية وحيث إن الضرب الداخلي هو الضرب النقطي المعتاد.

٩ - لتكن V مجموعة جميع الدوال الحقيقية $y=f(x)$ التي تحقق المعادل التفاضلية

$$\frac{d^2y}{dx^2}+9y=0$$

(ا) برهن على أن V فضاء متجهات حقيقي ثنائي البعد

(ب) عرف في V الضرب الداخلي : $(y,z)=\int_0^{\pi}yz\,dx$ ، أوجد أساسا متعامدا معايرا في V

١٠ - لتكن V مجموعة جميع الدوال الحقيقية $y=f(x)$ التي تحقق المعادل التفاضلية

$$\frac{d^3y}{dx^3}-6\frac{d^2y}{dx^2}+11\frac{dy}{dx}-6y=0$$

(ا) برهن على أن V فضاء متجهات ثلاثي البعد.

(ب) في V عرف

$$(u,v)=\int_{-\infty}^{0} uv\,dx$$

بين أن هذا يعرف ضربا داخليا على V ثم أوجد أساسا متعامدا معايرا في V.

١١ - إذا كان W فضاء جزئيا في V وكان v في V يحقق $(v,w)+(w,v)\leq(w,w)$ لكل w في W. فبرهن على أن $(v,w)=0$ لكل w في W.

١٢ - إذا كان V فضاء ضرب داخلي منتهي البعد وكان f داليًّا خطيًّا على V (أي f في $\hat{V}$) فبرهن على أنه يوجد u_0 في V بحيث: $f(v)=(v,u_0)$ لكل v في V.

(٤-٥) الفضاءات الحلقية

إن مفهوم الفضاء الحلقي هو تعميم لمفهوم فضاء المتجهات فبدلا من قصر القياسات على كونها عناصر في حقل بجعلها عناصر في حلقة اختيارية.

إن هذا البند يحوي العديد من التعاريف بالإضافة إلى مبرهنة واحدة فقط. إن التعاريف المذكورة في هذا البند ذات طبيعة قريبة من تعاريف سبق وأن ذكرناها في موضوع فضاءات المتجهات لذا فإن الأفكار الرئيسة التي سنتطرق إليها أدناه ينبغي ألا تنطمس تحت زحام هذه التعاريف.

تعريف

لتكن R حلقة، تدعى المجموعة غير الخالية M ***فضاءً حلقيًّا لـ R*** *(R-module) (أو فضاءً حلقيًّا على R) إذا كانت M زمرة إبدالية بالنسبة لعملية + بحيث لكل r في R و m في M يوجد عنصر rm في M يحقق الشروط التالية:*

١ - $r(a+b)=ra+rb$

٢ - $r(sa)=(rs)a$

٣ - $(r+s)a=ra+sa$

لجميع b,a في M و r ، s في R.

إذا كان للحلقة R عنصر وحدة 1 وكان 1m=m لجميع العناصر m في M فعندئذ يدعى M **فضاءً حلقيًّا واحديًّا** (unital module). لاحظ أنه إذا كانت R حقلا فالفضاء الحلقي الواحدي على R ليس إلا فضاء متجهات على R. *في دراستنا هذه كل الفضاءات الحلقية ستكون واحدية.*

إن الفضاء الحلقي الذي عرفناه أعلاه هو في الحقيقة فضاء حلقي أيسر على R ذلك لأننا ضربنا بعناصر R من اليسار. بصورة مشابهة يمكننا تعريف الفضاء الحلقي الأيمن على R. في شرحنا أدناه سوف لا نذكر صفة الأيمن والأيسر لأننا سنعنى بكلمة فضاء حلقي على R الفضاء الحلقي الأيسر على R.

مـــثـــال (٤-٥-١)

كل زمرة إبدالية G هي فضاء حلقي على حلقة الأعداد الصحيحة. كي تدرك ذلك اكتب عملية G على الشكل + ودع na لعنصر a في G و n عدد صحيح تدل على ما أشرنا إليه في الفصل الثاني. إن القواعد المعتادة للأسس في الحلقة الإبدالية تترجم نفسها إلى الخصائص التي نحتاجها كي تجعل في G فضاء حلقيا على حلقة الأعداد الصحيحة، لاحظ أيضا أنه فضاء حلقي واحدي.

مـــثـــال (٤-٥-٢)

لتكن R أية حلقة و M مثاليا أيسر في R. لعنصر r في R و m في M دع rm تساوي حاصـل ضرب هذين العنصرين كعناصر في R. إن تعريف المثالي الأيسر يقتضي أن يكون rm في M وأن المسلّمات التي تعرف الحلقة تجعل من M فضاءً حلقيًّا على R. (في هذا المثال الحلقة R يجب أن تكون تجميعية كي يكون r(sm)=(rs)m).

مـثـال (٤-٥-٣)

إن الحالة الخاصة التي فيها M=R تكون فيها أية حلقة R فضاءً حلقيًا على نفسها.

مـثـال (٤-٥-٤)

لتكن R أية حلقة و مثاليا أيسراً في R. لتكن M مجموعة المجموعات المشاركة $a+\lambda$ حيث a في R عرف

$$r(a+\lambda)=ra+\lambda \quad \text{و} \quad (a+\lambda)+(b+\lambda)=(a+b)+\lambda$$

وهـذا يجـعل M فضـاءً حلقـيًا عـلى R (انـظر مسألـة ٢ في نهـاية هذا البـند). يرمـز لـ M بالرمـز $R-\lambda$ (أو في بعـض الأحـيان R/λ) ويطلق عليه اسم **فضاء الفرق الحلقي** (difference module) أو **الفضـاء الحلـقي الخـارج** (quotient module) للحلقـة R بواسطة λ.

يطلق على زمرة الجمع الجزئية A لفضاء حلقي M على R اسم فضاء حلقي جزئي من M إذا كان ra في A لكل r في R و a في A.

إذا كان لدينا فضاء حلقي M على R وفضاء حلقي جزئي A يمكننا أن ننشىء الفضاء الحلقي الخارج بطريقة مشابهة لتلك التي استعملناها لانشاء الزمر الخارجية، الحلقات الخارجة والفضاءات الخارجة. كذلك يمكننا التحدث عن التشاكلات من فضاء حلقي على R إلى آخر وإثبات مبرهنات التشاكل المناسبة لذلك . هذا هو فحوى بعض المسائل في نهاية هذا البند. إن اهتمامنا بالفضاءات الحلقية يأخذ اتجاها مختلفا فسوف نحاول أن تجد تعريفا لفضاءات حلقية على حلقات معيّنة.

تعريف

*إذا كان M فضـاء حلقيا على R وكانت $M_1,\ldots,M_s$ فضاءات حلقية جزئية من M فيقـال عن M إنـه **الجمـع المباشر** (direct sum) لـ $M_1,\ldots,M_s$ إذا أمكن كتابة كل*

عنصر m في M بصورة وحيدة على الصيغة $m=m_1+m_2+...+m_s$ حيث m_1 في M_1 ، m_2 في M_2 ، . . . ، m_s في M_s.

كما هي الحال في فضاءات المتجهات إذا كان M الجمع المباشر لـ $M_1,...,M_s$ فإن M يماثل، كفضاء حلقي، مجموعة العديدات $(m_1,...,m_s)$ من رتبة s (s-tuples) حيث إن المركبة m_i هي أي عنصر في M_i وعملية الجمع تعرف بجمع المركبات.
وحيث $r(m_1,...,m_s)=rm_1+rm_2+...+rm_s$ لكل عنصر r في R من معرفة بناء كل M_i يمكننا أن نتعرف على بناء M.

إن الفضاءات الحلقية المولدة من عنصر واحد بسيطة وذات أهمية خاصة تطلق عليها اسم **فضاءات حلقية دورية** (cyclic modules) وتوخيا للدقة نعرف ما يلي.

تعريف

*يوصف الفضاء الحلقي M على R بأنه **دوري** (cyclic) إذا وجد عنصر m_0 في M بحيث لكل m في M ، $m=rm_0$ حيث r في R.*

في حالة كون R حلقة الأعداد الصحيحة يكون الفضاء الحلقي الدوري على R زمرة دورية.

بقي علينا تعريف واحد وهو ما يلي.

تعريف

*يقال عن الفضاء الحلقي على R إنه منتهي **التوليد** (finitely generated) إذا وجدت عناصر $a_1,...,a_n$ في M بحيث كل m في M هو على الصيغة $m=r_1a_1+r_2a_2+...+r_na_n$*

بعد تقديم التعاريف اللازمة نأتي الآن على المبرهنة التي تعتبر السبب الرئيس وراء وجود هذا البند. من الشائع أن يطلق على هذه المبرهنة اسم **المبرهنة الأساسية**

للفضاءات الحلقية المنتهية التوليد (The fundamental theorem on finitely genrated modules) على الحلقات الإقليدية في هذه المبرهنة ستقصر R على كونها حلقة إقليدية (الفصل الثالث، البند ٣-٧) ولكن في الواقع أن المبرهنة صحيحة في حالة أعم من ذلك عندما تكون R حلقة تامة رئيسة المثالي.

مبرهنة (٤-٥-١)

لتكن R حلقة إقليدية عندئذ أي فضاء حلقي M منته التوليد على R عبارة عن جمع مباشر لعدد منتهٍ من الفضاءات الحلقية الجزئية الدورية.

البرهان

قبل أن نخوض بتفاصيل البرهان لننظر إلى ما تقوله المبرهنة. إن الفرضية بكون M منته التوليد تفيدنا بوجود مجموعة من العناصر $a_1,...,a_n$ في M بحيث يمكن التعبير عن كل عنصر في M على الصيغة $r_1a_1+r_2a_2+...+r_na_n$ حيث r_i في R.

أما الاستنتاج في المبرهنة فيقول إنه تحت شروط مناسبة على R يمكن إيجاد مجموعة أخرى من العناصر $b_1,...,b_q$ في M بحيث من الممكن التعبير عن أي عنصر m في M بصورة وحيدة على الصيغة $m=s_1b_1+...+s_qb_q$ حيث s_i في R.

ثمة ملاحظة عن الوحدانية هنا، إنها لا تعني أن كل s_i وحيد، في الحقيقة إن هذا يمكن أن يكون غير صحيح. إن ما تعنيه المبرهنة أن العناصر s_ib_i وحيدة. أي إذا كان $m=s_1b_1+...+{}_qb_q$ و $m=s_1'b_1+...+s_q'b_q$ فلا يمكننا الاستنتاج أن $s_1=s_1'$ ، $s_2=s_2'$ ، . . . ، $s_q=s_q'$ ولكن يمكن أن نقول إن $s_1b_1=s_1'b_1$ ، . . . ، $s_qb_q=s_q'b_q$.

وملاحظة أخرى قبل أن نبدأ بالبرهان. بالرغم من أن المبرهنة تشير إلى الحلقة الاقليدية بصيغتها العامة إلا أننا سوف نعطي تفاصيل البرهان في حالة خاصة وهي حلقة الأعداد الصحيحة. في نهاية البرهان سوف نشير إلى التغيرات اللازم إجراؤها كي

يكون البرهان صالحا للحالة العامة. لقد اخترنا هذا السبيل لتجنب تداخل الأفكار الأساسية الذي قد يؤدي إلى الإرباك، بالإضافة إلى كون هذه الأفكار هي ذاتها التي تستخدم في الحالة العامة مع توخي بعض أوجه الدقة التي لا تبدو ذات أهمية.

وهكذا فإننا ببساطة نفترض أن M زمرة إبدالية ذات مجموعة توليد منتهية. لندعو مجموعات التوليد التي تحوي أقل عدد ممكن من العناصر **مجموعات توليد دنيا** (minimal generating sets) وندعو عدد العناصر في مجموعة توليد دنيا **مرتبة** (rank) M

الآن نبدأ البرهان بالاستقراء على مرتبة M:

إذا كانت مرتبة M تساوي 1 فإن M مولد بعنصر واحد مما يجعله دوريا وفي هذه الحالة تكون المبرهنة صحيحة. لنفرض أن النتيجة صحيحة لجميع الزمر الإبدالية من مرتبة $q-1$ وأن مرتبة M تساوي q. لتكن $a_1,\ldots,a_q$ مجموعة مولدة دنيا في M. لو كان $n_1a_1+n_2a_2+\ldots+n_qa_q=0$ (حيث $n_1,\ldots,n_q$ أعداد صحيحة) تقتضي أن يكون $n_1a_1=n_2a_2=\ldots=n_qa_q=0$ لأصبح M يساوي الجمع المباشر لـ $M_1,M_2,\ldots,M_q$ حيث M_i هو الفضاء الحلقي الدوري المولد (أو بالأحرى الزمرة الجزئية المولّدة) بواسطة a_i وبذلك ينتهي البرهان. ونتيجة لذلك، إذا كانت $b_1,\ldots,b_q$ مجموعة مولدة دنيا في M فيجب أن يكون هناك أعداد صحيحة $r_1,\ldots,r_q$ بحيث $r_1b_1+\ldots+r_qb_q=0$ وليس كل العناصر $r_1b_1,r_2b_2,\ldots,r_qb_q$ تساوي صفرا. من بين جميع هذه العلاقات للمجموعات المولدة الدنيا، يمكن إيجاد عدد صحيح موجب أدنى كمعامل في إحدى العلاقات. ليكن هذا العدد الصحيح s_1 والمجموعة المولدة التي يقع فيها كمعامل لأحد عناصرها هي $a_1,\ldots,a_q$ لذلك:

$$s_1a_1+s_2a_2+\ldots+r_qa_q=0 \quad (١)$$

إننا ندعي بأنه إذا كان $r_1a_1+\ldots+r_qa_q=0$ فإن $s_1|r_1$ ذلك لأن $r_1=ms_1+t$، $0\leq t<s_1$، وبضرب المعادلة (١) بالعدد m وطرحها من المعادلة $r_1a_1+\ldots+r_qa_q=0$ نحصل على: $ta_1+(r_2-ms_2)a_2+\ldots+(r_q-ma_q)a_q=0$ وبما أن $t<s_1$ و s_1 هو أصغر عدد صحيح موجب في مثل هذه العلاقة، لذا يجب أن يكون $t=0$.

أما الآن فندعي أن $s_1|s_i$ لكل $i=2,\ldots,q$ لنفرض أن هذا غير صحيح عندئذ $s_1 \nmid s_2$ مثلا، لذا: $s_2=m_2s_1+t$ ، $0<t<s_1$. إن العناصر $a_1'=a_1+m_2a_2,a_2,\ldots,a_q$ تولد M أيضا، ولكن $s_1a_1'+ta_2+s_3a_3+\ldots+s_qa_q=0$ ولذا فإن t يقع كمعامل في علاقة ما، بين عناصر مجموعة مولدة دنيا، ولكن هذا يجعل $t=0$ أو $t\geq s_1$ من اختيارنا للعدد s_1 إذن يجب أن يكون $t=0$ وبالتالي $s_1|s_2$ وهكذا بالنسبة لبقية المعاملات s_i. لنكتب $s_i=m_is_1$.

الآن لننظر إلى العناصر $a_1^*=a_1+m_2a_2+m_3a_3+\ldots+m_qa_q,a_2,\ldots,a_q$ إنها تولد M وبالاضافة إلى ذلك:

$$s_1a_1^*=s_1a_1+m_2s_1a_2+\ldots+m_q s_1a_q=s_1a_1+s_2a_2a+\ldots+s_qa_q=0$$

إذا كان $r_1a_1^*+r_2a_2+\ldots+r_qa_q=0$ فبالتعويض عن a_1^* نحصل على علاقة بين $a_1,\ldots,a_q$ فيها معامل a_1 يساوي r_1 مما يجعل $s_1|r_1$ وبالتالي $r_1a_1^*=0$. إذا كان M_1 الفضاء الحلقي الجزئي الدوري المولد بواسطة a_1^*. و M_2 الفضاء الحلقي الجزئي من M المولد بواسطة $a_2,\ldots,a_q$ فنكون قد برهنا على أن $M_1\cap M_2=(0)$. ولكن $M_1+M_2=M$ لأن $a_1^*,a_2,\ldots,a_q$ تولد M. نستنتج أن M يساوي الجمع المباشر لـ M_1 و M_2. ولما كان M_2 مولدا بواسطة $a_2,\ldots,a_q$ فإن مرتبته لا تزيد عن $q-1$ (في الحقيقة إنها تساوي $q-1$) لذا فوفقا للاستقراء يصبح M_2 حاصل الجمع المباشر لفضاءات حلقية دورية. بجمع كل ما حصلنا عليه أعلاه، نجد أنه يمكن تفريق M إلى حاصل جمع مباشر لفضاءات حلقية دورية.

نتيجة

كل زمرة إبدالية منتهية هي حاصل ضرب (جمع) مباشر لزمر دورية.

البرهان

من البديهي أن الزمرة الإبدالية المنتهية هي منتهية التوليد، في الواقع إنها مولدة من المجموعة المنتهية الحاوية على جميع عناصر الزمرة. لذا فوفقا للمبرهنة **(٤-٥-١)** نحصل على النتيجة. طبعا، هذه نفس النتيجة التي أثبتناها في مبرهنة **(٢-١٤-١)**.

الآن نفرض أن R حلقة إقليدية مع الدالة d. نقوم بإجراء التعديلات اللازمة على البرهان المعطى في حالة الأعداد الصحيحة كي يصلح لـ R كالتالي:

١ - بدلا من اختيار s_1 كأصغر عدد صحيح موجب يقع كمعامل في أية علاقة بين عناصر مجموعة مولدة دنيا، اختره كعنصر من R يقع في أية علاقة بحيث تكون قيمة d له أصغر ما يمكن.

٢ - في البرهان إن $s_1|r_1$ لأية علاقة $r_1a_1+...+r_qa_q=0$ ، إن التغيير اللازم هو $r_1=ms_1+t$ حيث إما $t=0$ أو $d(t)<d(s_1)$. أما بقية التفاصيل فتبقى كما هي. وبصورة مشابهة نجري التعديل في برهان أن $s_1|s_i$.

وهكذا نجد أنه بإجراء التعديلات البسيطة هذه يكون البرهان صحيحا في حالة الحلقات الاقليدية العامة وتكون بذلك قد أكملنا إثبات المبرهنة (٤-٥-١).

مسائل

١ - تحقق من صحة المذكور في المثال (٤-٥-١) حول كون كل زمرة إبدالية فضاءً حلقيًا على حلقة الأعداد الصحيحة.

٢ - تحقق من أن المجموعة المذكورة في مثال (٤-٥-٤) تكوِّن فضاءً حلقيًا على R.

٣ - لنفرض أن R حلقة بعنصر وحدة و M فضاء حلقي غير واحدي على R. برهن على وجود عنصر $m\neq0$ في M بحيث $rm=0$ لكل r في R.

*إذا كان M و N فضاءين حلقيين على R و T تطبيقا من M إلى N ، يطلق على T اسم **تشاكل** (homomorphism) أو **تشاكل على R** (R-homomorphism) أو **تشاكل فضاء حلقي** (module homomorphism) إذا كان:*

١ - $(m_1+m_2)T=m_1T+m_2T$

٢ - $(rm_1)T=r(m_1T)$

لكل m_1 و m_2 في M و r في R.

٤ - إذا كان T تشاكلا من M إلى N وكان $K(T)=\{x\in M|xT=0\}$. برهن على أن K(T) فضاء حلقي جزئي من M وأن $I(T)=\{xT|x\in M\}$ فضاء حلقي جزئي من N.

٥ - يطلق على التشاكل T اسم **تماثل** إذا كان أحاديا . برهن على أن T تماثل إذا وفقط إذا كانت $K(T)=0$.

٦ - ليكن M ، N و Q ثلاثة فضاءات حلقية على R ، T تشاكلا من M إلى N و S تشاكلا من N إلى Q. عرف $TS:M\to Q$ بواسطة $m(TS)=(mT)S$ لكل m في M.
برهن على أن TS تشاكل من M إلى Q ثم حدد نواته $K(TS)$.

٧ - إذا كان M فضاءً حلقيًا على R و A فضاءً حلقيًا جزئيًا من M ، عرِّف الفضاء الخارج M/A (باستعمال نفس الأسلوب المتبع في الزمر، الحلقات وفضاءات المتجهات) بحيث يكون فضاءً حلقيًا على R. برهن على وجود تشاكل من M على M/A.

٨ - إذا كان T تشاكلا من M على N و $K(T)=A$. فبرهن على أن N يماثل (كفضاء حلقي) M/A.

٩ - إذا كان A و B فضاءين حلقيين جزئيين من M فبرهن على أن :
(ا) $A\cap B$ فضاء حلقي جزئي من M
(ب) $A+B=\{a+b|a\in A,b\in B\}$ فضاء حلقي جزئي من M.
(جـ) $(A+B)/B$ يماثل $A/A\cap B$

١٠ - يقال عن فضاء حلقي على R إنه غير مختزل إذا كان لا يحوي فضاءات حلقية جزئية سوى (0) و M. برهن على أن كل فضاء حلقي واحدي غير مختزل على R يجب أن يكون دوريا .

١١ - إذا كان فضاءً حلقيًا غير مختزل على R. فبرهن على أنه إما أن يكون M دوريا أو لجميع m في M و r في R ، $rm=0$.

١٢* - إذا كان M فضاء حلقيا غير مختزل على R بحيث إن $rm\neq 0$ لعنصر ما r في R و m في M. فبرهن على أن أي تشاكل T من M إلى نفسه هو إما تماثل من M على نفسه أو $mT=0$ لجميع m في M.

١٣ - ليكن M فضاءً حلقيًا على R و $E(M)$ مجموعة جميع التشاكلات من M إلى نفسه .
عرف عمليتي جمع وضرب مناسبتين على $E(M)$ لتجعل منها حلقة . (إرشاد : قلد ما عُمل في حالة $Hom(V,V)$ حيث V فضاء متجهات) .

١٤* - إذا كان M فضاءً حلقيًّا غير مختزل على R بحيث $rm \neq 0$ لعنصر ما r في R و m في M. فبرهن على أن E(M) حلقة قسمة (تدعى هذه النتيجة **بتمهيدية شور** (Schur's lemma

١٥ - أعط برهـانا كاملا للمبرهنة (٤-٥-١) للفضاءات الحلقية المنتهية التوليد على الحلقات الاقليدية .

١٦ - ليكن M فضاءً حلقيًّا على R. إذا كان m في M وكان $\lambda(m)=\{x\in R|xm=0\}$. فبين أن $\lambda(m)$ مثالي أيسر في R. يُطلق عليه اسم **رتبة** m (order).

١٧ - إذا كان λ مثاليا أيسر في R و M فضاء حلقيا على R. فبيّن أنه بعنصر m في M يكون $\lambda m=\{xm|x\in\lambda\}$ فضاءً حلقيًّا جزئيًّا من M.

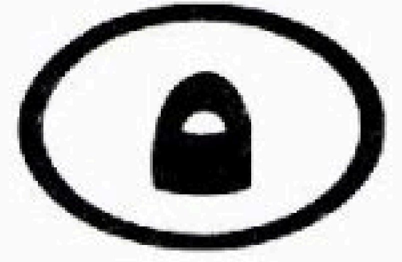
١٨* - ليكن M فضـاءً حلقيًّا غير مختزل على R وفيه $rm\neq 0$ لعنصر ما r في R و m في M. للعنصر $m_0\neq 0$ دع $\lambda(m_0)=\{x\in R|xm_0=0\}$

(ا) برهن على أن $\lambda(m_0)$ مثالي أيسر أعظمي في R (أي إذا كان λ مثاليا أيسر في R بحيث $R\supset\lambda\supset\lambda(m_0)$ فإما أن يكون $\lambda=R$ أو $\lambda=\lambda(m_0)$).

(ب) برهن على أن الفضاءين الحلقيين M و $R-\lambda(m_0)$ على R متماثلان [انظر مثال (٤-٥-٤)].

قراءة إضافية

Halmos, Paul R. *Finite-Dimensional Vector Spaces*. 2^{nd} Ed. Princeton, N.J.: D. Van Nostrand Company, Inc., 1958.



الحقول

● امتداد الحقول ● تسامي العدد e ● جذور كثيرات الحدود ● الانشاء الهندسي باستعمال المسطرة والفرجار ● المزيد عن الجذور ● مبادىء نظرية جالوا ● قابلية الحل باستخلاص الجذور ● زمر جالوا على حقل الأعداد النسبية

لقد سبق وأن أشرنا إلى الحقول كحالة خاصة من الحلقات أثناء دراستنا لها. ولنتذكر أن الحقل هو حلقة إبدالية بعنصر وحدة بحيث يوجد معكوس ضربي لكل عنصر لا يساوي صفرا، وبعبارة أخرى، الحقل هو حلقة إبدالية يمكن فيها التقسيم على أي عنصر غير صفري.

إن للحقول دورا مهما في الجبر ويعود ذلك إلى عدة أسباب منها استخدام بعض النتائج في نظرية الأعداد. وسبب آخر أن نظرية الحقول تتضمن نظرية المعادلات التي تعالج أسئلة تتعلق بجذور المعادلات.

في دراستنا هذه سوف لا ندخل في تفاصيل حقل الأعداد الجبرية وبدلا من ذلك سيكون تركيزنا على جوانب نظرية الحقول المتعلقة بنظرية المعادلات. على الرغم من أن معالجتنا للمادة سوف لا تكون في صورتها العامة والكاملة ولكن ستكون كافية لتقديم بعض الأفكار الشيّقة التي تعود إلى عالم الرياضيات الفرنسي إيفارست جالوا (Evariste Galois) والتي لها الأثر البالغ في الجبر الذي ندرسه اليوم.

(٥ـ١) امتداد الحقول

في هذا البند سنعنى بعلاقة حقل مع آخر. فليكن F حقلا، يدعى الحقل K **امتدادا** (extension) للحقل F إذا احتوى K الحقل F. وبعبارة مكافئة يكون K امتدادا لـ F إذا كان F حقلا جزئيا من K *(في هذا الفصل F يرمز إلى حقل ما و K إلى امتداد له)*.

كما سبق وأن ذكر في فصل فضاءات المتجهات، إذا كان K امتدادا لـ F فنسبة إلى عمليات الحقل الاعتيادية في K يكون K فضاء متجهات على F. وكفضاء متجهات يمكننا التحدث عن الارتباط الخطي، البعد والأساس. . . الخ في K نسبة إلى F.

تعريف

تعرف درجة (degree) K على F على أنها بعد K كفضاء متجهات على F.

سنرمز دائما إلى درجة K على F بالرمز [K:F]. وسنهتم بالحالة التي يكون فيها [K:F] عددًا منتهيًا، أي في حالة كون K منتهي البعد كفضاء متجهات على F. نصف هذه الحالة بقولنا إن K امتداد منته لـ F.

نبدأ أولاً بمبرهنة في حالة الامتداد المنتهي، هي سهلة نسبيا ولكنها ذات فائدة كبرى.

مبرهنة (٥ـ١ـ١)

إذا كان L امتدادا منتهيا لـ K و K امتدادا منتهيا لـ F فإن L امتداد منته لـ F وبالاضافة إلى ذلك [L:F]=[L:K][K:F]

البرهان

إن طريقة البرهان ستكون بكتابة أساس معين للحقل L على F. بهذه الطريقة إننا لا نثبت أن L امتداد منته لـ F فحسب ولكن في الحقيقة نبرهن على النتيجة الأعمق التي تعتبر عصب هذه المبرهنة وهي [L:F]=[L:K][K:F]

لنفرض إذن أن $[L:K]=m$ و $[K:F]=n$ ودع $v_1,\dots,v_m$ يكون أسـاسا لـ L على K و $w_1,\dots,w_n$ أساسا لـ K على F. ألا تعتقد أنه من الطبيعي أن تكون العناصر v_iw_j حيث $i=1,2,\dots,m$ و $j=1,2,\dots,n$ أساس لـ L على F ؟ على الأقل إن عدد هذه العناصر هو العدد الذي ننشده.

الآن نبدأ ببرهان أن هذه العناصر تكون أساسا لـ L على F.

أولا يجب أن نبيّن أن كل عنصر في L هو تركيب خطي من هذه العناصر بمعاملات في F ومن ثم نثبت أن هذه العناصر التي عددها mn مستقلة خطيا على F. ليكن t عنصرا ما في L. لما كان كل عنصر في L هو تركيب خطي من $v_1,\dots,v_m$ بمعـامـلات في K فكـذلـك t. أي أن $t=k_1v_1+\dots+k_mv_m$ حيث $k_1,\dots,k_m$ في K. ولكن كل عنصر في K هو تركيب خطي من $w_1,\dots,w_n$ بمعاملات في F مما يجعل

$$k_1=f_{11}w_1+\dots+f_{1n}w_n\ ,\dots,\quad k_i=f_{i1}w_1+\dots+f_{in}w_n,\quad \dots, k_m=f_{m1}w_1+\dots+f_{mn}w_n.$$

حيث جميع f_{ij} في F.

بالتعويض عن عبارة كل من $k_1,\dots,k_m$ في $t=k_1v_1+\dots+k_mv_m$ نحصل على

$$t=(f_{11}w_1+\ \dots+f_{1n}w_n)v_1+\dots+(f_{m1}w_1+\dots+f_{mn}w_n)v_m$$

باستخدام قانوني التوزيع والتجميع يمكننا كتابة t على الشكل:

$$t=f_{11}v_1w_1+\dots+f_{1n}v_1w_n+\ \dots+f_{ij}v_iw_j+\dots+f_{mn}\ w_n.$$

ولما كانت العناصر f_{ij} في F نكون قد عبّرنا عن t كتركيب خطي على F من العناصر v_iw_j.
لذا فإن العناصر v_iw_j تولـد L على F وتحقق بذلك الشرط الأول في كونها أساسا.
يبقى أن نبين أن العناصر v_iw_j مستقلة خطيا على F. نفرض أن

$$f_{11}v_1w_1+\dots+f_{1n}v_1w_n+\ \dots+f_{ij}v_iw_j+\dots+f_{mn}v_mw_n=0$$

حيث f_{ij} في F. إن هدفنا هو إثبات أن $f_{ij}=0$. ومن أجل ذلك نعيد تجميع العبارة أعلاه فنحصل على:

$$(f_{11}w_1+\dots+f_{1n}w_n)\quad v_1+\dots+(f_{i1}w_1+\dots+f_{in}w_n)v_i+\dots+\ (f_{m1}w_1+\dots+f_{mn}w_n)v_m=0$$

ولما كانت w_i في K و $K\supset F$ فإن جميع العناصر $k_i=f_{i1}w_1+\dots+f_{in}w_n$ في K.

الآن $k_1v_1+\ldots+k_mv_m=0$ حيث $k_1,\ldots,k_m$ في K ولكن $v_1,\ldots,v_m$ تكون أساسا لـ L على K مما يجعلها مستقلة خطيًا على K وهذا يؤدي إلى أن $k_1=k_2=\ldots=k_m=0$.
وبالتعويض عن k_i نحصل على

$$f_{i1}w_1+\ldots+f_{in}w_n=0$$

لجميع قيم $i=1,2,\ldots,m$. ولكن w_i مستقلة خطيًا على F مما يؤدي إلى أن $f_{ij}=0$. وبذلك نكون قد برهنا على أن العناصر v_iw_j مستقلة خطيًا على F وبناءً عليه تكون هذه العناصر قد استوفت الشرط الثاني كي تكون أساسا.

لقد نجحنا في برهان أن العناصر v_iw_j والتي عددها mn تكون أساسًا لـ L على F. لذا $[L:F]=mn$ ، ولما كان $m=[L:K]$ و $n=[K:F]$ نحصل على النتيجة التي ننشدها، وهي $[L:F]=[L:K][K:F]$.

الآن لنفرض أن $L\supset K\supset F$ حيث L,K,F ثلاثة حقول وأن $[L:F]$ منته.
من الواضح أن أية مجموعة من العناصر في L مستقلة خطيا على K تكون بطبيعة الحال مستقلة خطيًا على F. لذا فإن الفرض بأن $[L:F]$ منته يدعونا لاستنتاج أن $[L:K]$ منته. ومن ناحية أخرى لما كان K فضاءً جزئيًا من L يكون $[K:F]$ منتهيا. وفقا للمبرهنة نحصل على $[L:F]=[L:K][K:F]$ مما يجعل $[K:F]|[L:F]$ وبذا نكون قد برهنّا على النتيجة.

نتيجة:

إذا كان L امتدادًا منتهيًا لـ F و K حقلا جزئيا من L يحوي F ، فإن $[K:F]|[L:F]$.

وهكذا، فعلى سبيل المثال إذا كان $[L:F]$ عددًا أوليًا فلا يمكن أن يوجد حقل يقع فعليا بين F و L. عندما ندرس موضوع إنشاء بعض الأشكال الهندسية باستعمال المسطرة والفرجار في بند (٥-٤) سيكون لهذه النتيجة أهمية كبرى.

تعريف

يقال عن عنصر a في K إنه جبري (algebraic) على F إذا وُجدت عناصر $\alpha_0,\alpha_1,\ldots,\alpha_n$ في F ليست جميعها صفرا بحيث $\alpha_0a^n+\alpha_1a^{n-1}+\ldots+\alpha_n=0$.

إذا كانت F[x] هي حلقــة كثـيرات الحــدود في x على F وكانت $q(x)\in F[x]$ حيث $q(x)=\beta x^m+\beta_1x^{m-1}+\ldots+\beta_m$ فإنــه لأي عنصر b في K سنعنى بـ q(b) العنصر $\beta_0b^m+\beta_1b^{m-1}+\ldots+\beta_m$ في K. إن العبارة الشائعة هي أن q(b) قيمة كثيرة الحدود q(x) عندما نعوض عن x بالعنصر b. ويقال إن العنصر b **يحقق (satisfy)** q(x) إذا كان q(b)=0. باستخدام هذا الأسلوب يكون a في K جبريًا على F إذا وُجدت كثيرة حدود غير صفرية p (x) في F [x] بحيث إن العنصر a يحققها أي يكون p (a)=0 .

ليكن K امتدادًا لـ F و a في K. ولتكن M مجموعة جميع الحقول الجزئية من K والتي تحتوي كلا من F و a. M لا تساوي المجموعة الخالية ذلك لأن K في M. من السهل البرهان على أن تقاطع أي عدد في الحقول الجزئية من K هو أيضا حقل جزئي في K. لذا فإن تقاطع الحقول الجزئية من K والموجودة في M هو حقل جزئي من K نرمز له بالرمز F(a). ونسأل: ما هي خواص هذا الحقل؟ من المؤكد أنه يحوي a و F لأن هذا صحيح بالنسبـة لجميع الحقول الجزئية من K الموجودة في M. وإضافة إلى ذلك ومن تعريف التقاطع فإن أي حقل جزئي من K في M يحوي F(a). ولكن F(a) نفسه موجود في M مما يجعـل F(a) **أصغر حقل جزئي من K يحتوي على كل من F و a.** وندعو F(a) **الحقل الجزئي المتكون من ضم a إلى F.**

إن وصفنا للحقل F(a) حتى الآن كان وصفا خارجيا. أما الآن فنقدِّم وصفا بديلا لـ F(a) ذا طبيعـة إنشـائية. لننظر إلى جميع عناصر K التي يمكن كتابتها على الصيغـة $\beta_0+\beta_1a+\ldots+\beta_sa^s$ حيث b_i عنـاصر اختيارية في F و s أي عدد صحيح غير سالب. كعناصر في K يمكن تقسيم أي عنصر من هذا النوع على آخر بشرط أن لا يكون العنصر الأخير صفرا. لتكن U مجموعة جميع خوارج القسمة هذه. نترك للقارىء

كتمرين البرهان على أن U حقل جزئي من K. من الواضح أن الحقل U يحوي F و a مما يجعل $U \supset F(a)$. ومن جهة أخرى كل حقل جزئي من K يحوي كلا من F و a يجب أن يحوي جميع العناصر التي على الصيغة $\beta_0+\beta_1 a+\ldots+\beta_s a^s$ حيث β_i في F وذلك لانغلاقه تحت عمليتي الجمع والضرب. لذا فإن F(a) يجب أن يحوي جميع هذه العناصر، ولكونه حقلا جزئيًا من K فإنه يحوي خوارج قسمة مثل هذه العناصر، إذن $F(a) \supset U$. من العلاقتين $U \subset F(a)$ ، $U \supset F(a)$ نحصل على $F(a)=U$. بهذه الطريقة حصلنا على إنشاء داخلي لـ F(a) ، ألا وهو U.

الآن نربط بين خاصة كون a في K جبريًا على F والخواص المنظورة للحقل F(a) نفسه.

مبرهنة (٥-١-٢)

يكون العنصر a في K جبريًا على F إذا وفقط إذا كان F(a) امتدادًا منتهيًا للحقل F

البرهان

كما هو المعتاد في مثل هذه المبرهنة التي تحوي إذا وفقط إذا فإن إثبات أحد الاتجاهين، يكون سهلا غير معقد بينما يكون إثبات الاتجاه الآخر أكثر عمقًا وتعقيدًا.

لنفرض أن F(a) امتداد منته لـ F وأن $[F(a):F]=m$ ولننظر إلى العناصر $1,a,a^2,\ldots,a^m$ في F(a) والتي عددها m+1. وفقا لتمهيدية (٤-٢-٤) فإن هذه العناصر مرتبطة خطيًا على F. إذن توجد عناصر $\alpha_0,\alpha_1,\ldots,\alpha_m$ في F ليست جميعها صفرا بحيث $\alpha_0 1+\alpha_1 a+\alpha_2 a^2+\ldots+\alpha_m a^m=0$. لذا فإن a جبري على F ويحقق كثيرة الحدود غير الصفرية $p(x)=\alpha_0+\alpha_1 x+\ldots+\alpha_m x^m$ في F[x] والتي درجتها لا تتعدى $m=[F(a):F]$. هذا يثبت جزء «إذا» من المبرهنة وهو الشرط الكافي.

الآن نثبت جزء «إذا فقط» وهو الشرط الضروري من المبرهنة. لنفرض أن a في K جبري على F. لذا فإن a تحقق كثيرة حدود غير صفرية في F[x]. لتكن p(x) كثيرة الحدود

في $F[x]$ ذات الدرجة الموجبة الأصغر بحيث $p(a)=0$. إننا ندعي أن $p(x)$ غير مختزلة على F. فإذا كانت $p(x)=f(x)g(x)$ حيث $f(x)$ و $g(x)$ في $F[x]$ فإن $0=p(a)=f(a)g(a)$ (انظر مسألة ١). وحيث إن $f(a)$ و $g(a)$ عنصران في الحقل K نستنتج $f(a)=0$ أو $g(a)=0$. ولما كانت $p(x)$ ذات أصغر درجة موجبة بحيث $p(a)=0$ نستنتج أن $\deg f(x) \geqslant \deg p(x)$ أو $\deg g(x) \geqslant \deg p(x)$ وهذا يبرهن على أن $p(x)$ غير مختزلة على F.

الآن نعـرف التـطبيق ψ من $F[x]$ إلى $F(a)$ كما يلي: لكـل $h(x)$ في $F(x)$ دع $h(x)\psi = h(a)$. نترك للقارىء التحقق من أن ψ هو تشاكل من الحلقة $F[x]$ إلى الحقل $F(a)$ (انظر مسألة ١). ونسأل: ما هي نواة ψ التي نرمز لها بـ V ؟ من تعريف ψ، $V=\{h(x)\in F[x] | h(a)=0\}$. كذلك نجد أن $p(x)$ عنصر في V درجته أصغر ما يمكن. بالاستعانة بنتائج بند (٣-٩) نجد أن كل عنصر في V هو مضاعف لـ $p(x)$ ولكون $p(x)$ غير مختزلة فوفقا لتمهيدية (٣-٩-١) يكون V مثاليا أعظميا في $F[x]$. وبالاستعانة بمبرهنة (٣-٥-١) نحصـل على أن $F[x]/V$ حقـل. والآن وبـاستعمال مبرهنة التشاكل العامة للحلقـات (مـبرهنـة ٣-٤-١) يكـون $F[x]/V$ مماثـلا لصـورة $F[x]$ وفق التشـاكل ψ. فبـاختصار، أثبتنا أن صورة $F[x]$ وفق ψ هي حقل جزئي من $F(a)$. إن هذه الصورة تحوي $x\psi=a$ ولكل α في F ، $\alpha\psi=\alpha$. لذا فإن صورة $F[x]$ وفق ψ هي حقل جزئي من $F(a)$ يحوي كلا من F و a وباستعمال تعريف $F(a)$ نستنتج أن صورة $F[x]$ وفق ψ هي كل $F(a)$. وهكذا يكون $F[x]/V$ مماثلا لـ $F(a)$.

الآن ولكون $V=(p(x))$ المثالي المتولد من $p(x)$ ، ندَّعي أن بعد فضاء المتجهات $F[x]/V$ على F هو بالضبط درجـة $p(x)$ (انـظر مسـألـة ٢). وبـالنـظر للتـماثـل بين $F[x]/V$ و $F(a)$ نحصل على أن $[F(a):F]=\deg p(x)$. لذا يكون $[F(a):F]$ منتهيًا. وهذا ما نريد إثباته في جزء «فقط إذا» من المبرهنة. لاحظ أننا أثبتنا أكثر من ذلك وبالتحديد أن $[F(a):F]$ يساوي درجة كثيرة الحدود $p(x)$ التي درجتها أصغر ما يمكن بحيث $p(a)=0$.

إن البرهان الذي قُدم أعلاه كان مطوّلاً بعض الشيء، بيد أن هذا كان متعمدًا ذلك لأن الطريقة التي اتبعت تحوي أفكارًا مهمة وتربط نتائج ومفاهيم طُوِّرت آنفا مع

ما ندرسه الآن. وهذا غير مستغرب لأن الرياضيات لا تحوي مواضيع مستقلة تماما بحد ذاتها.

الآن نعيد برهان جزء «فقط إذا» بالعمل داخل الحقل $F(a)$. إن عملنا سيبدو، في الحقيقة، مطابقا للبرهان المقدم أعلاه ولكن الاختلاف يكمن في أن أجزاء البرهان مرتبة بشكل مختلف بعض الشيء.

مرة أخرى دع $p(x)$ كثيرة الحدود على F التي درجتها أقل ما يمكن بحيث $p(a)=0$. تدعى مثل كثيرة الحدود هذه **بكثيرة الحدود الدنيا (minimal polynomial) لـ a على F**. يمكننا الفرض أن معامل أعلى قوة لـ x هو 1 أي أنها واحدية؛ وفي هذه الحالة يمكننا التحدث عن كثيرة الحدود الدنيا لـ a على F ذلك لأن أي كثيرتي حدود واحديتين دنيوين لـ a على F متساويتين (برهن على ذلك). لنفرض أن درجة $p(x)$ تساوي n أي أن $p(x)=x^n+\alpha_1x^{n-1}+\ldots+\alpha_n$ حيث α_i في F. حسب افتراضنا يكون $a^n+\alpha_1a^{n-1}+\ldots+\alpha_n=0$ وبالتالي: $a^n=-\alpha_1a^{n-1}-\alpha_2a^{n-2}-\ldots-\alpha_n$. ماذا عن a^{n+1}؟

من العلاقة أعلاه $a^{n+1}=-\alpha_1a^n-\alpha_2a^{n-1}-\ldots-\alpha_na$ وإذا عوضنا عن a^n بما تساويه أعلاه في الجانب الأيمن من هذه العلاقة نحصل على a^{n+1} كتركيب خطي من العناصر $1,a,\ldots,a^{n-1}$ على F. وبالاستمرار على هذا النحو نحصل على a^{n+k} حيث $k\geqslant 0$ على شكل تركيب خطي على F من العناصر $1,a,\ldots,a^{n-1}$. الآن لننظر إلى

$$T=\{\beta_0+\beta_1a+\ldots+\beta_{n-1}a^{n-1}|\beta_0,\beta_1,\ldots,\beta_{n-1}\in F\}$$

من الواضح أن T مغلقة بالنسبة لعملية الجمع ومن الملاحظات أعلاه تكون T مغلقة بالنسبة لعملية الضرب أيضا. ومهما يكن فإن T هذه تشكل حلقة على الأقل. بالإضافة إلى ذلك، T تحتوي كلا من F و a. والآن نثبت أن T ليست حلقة فحسب وإنما هي حقل.

ليكن $0\neq u=\beta_0+\beta_1a+\ldots+\beta_{n-1}a^{n-1}$ في T و $h(x)=\beta_0+\beta_1x+\ldots+\beta_{n-1}x^{n-1}$ في $F[x]$. عندئذ لما كان $u\neq 0$ ولما كان $u=h(a)$ فإن $h(a)\neq 0$ وعليه فإن $p(x)\nmid h(x)$. وحيث إن $p(x)$

غير مختزلة لذا فإن $p(x)$ و $h(x)$ يجب أن تكونا أوليتين نسبيًا. لذا يمكننا إيجاد كثيرتي حدود $s(x)$ و $t(x)$ في $F[x]$ بحيث $p(x)s(x)+h(x)t(x)=1$. ولكن حينئذ

$$1=p(a)s(a)+h(a)t(a)=h(a)t(a)$$

لأن $p(a)=0$ ، و بالتعويض $u=h(a)$ نحصل على $ut(a)=1$. وبذا يكون $t(a)$ معكوس u ولاحظ أن قوى a في $t(a)$ التي تزيد عن $n-1$ يمكن استبدالها بتراكيب خطية من $1,a,\ldots,a^{n-1}$ على F مما يجعل $t(a)$ في T. لقد بيّنا أن لكل عنصر غير صفري في F معكوس في T ونتيجة لذلك يكون T حقلا. ولكن $T\subset F(a)$ وكل من a و F محتوٍ في T مما يؤدي إلى أن $T=F(a)$. بهذا نكون قد وصفنا $F(a)$ على أنه جميع العبارات على الصيغة $\beta_0+\beta_1a+\ldots+\beta_{n-1}a^{n-1}$.

لأن T مولـد على F من العناصر $1,a,\ldots,a^{n-1}$ مما يجعل $[T:F]\leqslant n$. ولكن العناصر $1,a,a^2,\ldots,a^{n-1}$ مستقلة خطيًّا على F لأن أية علاقة من الصيغة $\gamma_0+\gamma_1a+\ldots+\gamma_{n-1}a^{n-1}=0$ حيث γ_i في F تقودنا لاستنتاج أن a تحقق كثيرة الحدود $\gamma_0+\gamma_1x+\ldots+\gamma_{n-1}x^{n-1}$ على F والتي درجتها أقل من n. هذا التناقض يبرهن الاستقلالية للعناصر $1,a,\ldots,a^{n-1}$ وبذا تكون هذه العناصر أساسا لـ T على F وبناءً عليه يكون $[T:F]=n$. ولما كان $T=F(a)$ نحصل على $[F(a):F]=n$.

تعريف

يُدعى العنصر a في K جبريًّا من الدرجة n على F إذا حقق كثيرة حدود غير صفرية على F من الدرجة n ولا يحقق سواها من درجة أقل.

أثناء برهاننا لمبرهنة (٥-١-٢) (في كلا البرهانين) أثبتنا نتيجة أدق من تلك المذكورة في المبرهنة ألا وهي المبرهنة التالية.

مبرهنة (٥-١-٣)

إذا كان a في K جبريا من الدرجة n على F فإن $[F(a):F]=n$.

إن هذه النتيجة استعمالات عديدة أحدها الاستنتاج الشيق في المبرهنة التالية.

مبرهنة (٥-١-٤)

إذا كان a و b في K جبريين على F فإن كلا من a±b ، ab ، a/b (إذا كان b≠0) جبريًا على F. وبعبارة أخرى تكون العناصر الجبرية على F من الحقل K حقلاً جزئيا من K.

البرهان

لنفرض أن a جبري من الدرجة m على F و b جبري من الدرجة n على F. وفقا لمبرهنة (٥-١-٣) فإن درجة الحقل الجزئي T=F(a) في K على F تساوي m لكون b جبريًا على F من الدرجة n فمن الطبيعي أن يكون جبريًا من درجة لا تزيد عن n على T الذي يحتوي F. لذا فإن الحقل الجزئي W=T(b) من K ذو درجة لا تزيد عن n على الحقل T بالاستعانة بمبرهنة (٥-١-٣) مرة أخرى. ولكن [W:F]=[W:T][T:F] حسب مبرهنة (٥-١-١). إذن [W:F] ≤ mn مما يجعل W امتدادًا منتهيًا لـ F. بيد أن a و b في W لذا فإن a±b ، ab و a/b في W. بالاستعانة بمبرهنة (٥-١-٢) ولكون [W:F] منتهيًا تكون هذه العناصر جبرية على F مما يثبت المبرهنة.

هنا أيضا أثبتنا أكثر مما تذكره المبرهنة، فلكون [W:F[≤mn كل عنصر في W يحقق كثيرة حدود درجتها لا تزيد عن mn على F، ومن ذلك نحصل على النتيجة التالية.

نتيجة:

إذا كان a و b في K جبريين على F من الدرجة m و n على الترتيب، فإن a±b ، ab و a/b (إذا كان b≠0) عناصر جبرية على F درجاتها لا تزيد عن mn.

في برهاننا للمبرهنة السابقة كونا امتدادين للحقل F: **الأول** أسميناه T الذي يساوي F(a). **والثاني** W الذي يساوي T(b). لذا فإن W=F(a)(b). والمعتاد كتابته على

الصيغة $F(a,b)$. وبصورة مشابهة يمكننا التحدث عن $F(b,a)$. إنه ليس من الصعب البرهـان على أن $F(a,b)=F(b,a)$. على هذا المنـوال يمكننـا تعريف $F(a_1,a_2,\ldots,a_n)$ للعناصر $a_1,\ldots,a_n$ في K.

تعريف

- ***يطلق على الامتداد K لـ F امتداد جبري (algebraic extension) لـ F إذا كان كل عنصر في K جبريًا على F.***

الآن نبرهن حقيقة أخرى على نمط البراهين التي أثبتناها حتى الآن.

مبرهنة (٥-١-٥)

إذا كان L امتدادًا جبريًا لـ K و K امتدادًا جبريًا لـ F ، فإن L امتداد جبري لـ F.

البرهـــان

ليكن u عنصرًا اختياريًا في L. نريد أن نثبت أن u يحقق كثيرة حدود غير تافهة معاملاتها في F. ما هي المعلومات المتوفرة لدينا الآن؟ إننا نعلم أن u يحقق كثيرة حدود $x^n+\sigma_1 x^{n-1}+..+\sigma_n$ حيث $\sigma_1,\ldots,\sigma_n$ في K. ولكن K جبري على F لذا فبـاستعمال مبرهنة (٥-١-٣) عدة مرات يكون $M=F(\sigma_1,\ldots,\sigma_n)$ امتدادًا منتهيًا لـ F. لما كان u يحقق كثيرة الحدود $x^n+\sigma_1 x^{n-1}+\ldots+\sigma_n$ الذي معاملاتها في M لذا فإن u جبري على M. وفقا لمبرهنة (٥-١-٢) يكون $M(u)$ امتدادًا منتهيًا لـ M. ولكن بالاستعانة بمبرهنة (٥-١-١) فإن:

$$[M(u):F]=[M(u):M][M:F]$$

لذا فإن $M(u)$ امتداد منته لـ F. وهذا يقتضي أن يكون u جبريًا على F مما يكمل إثبات المبرهنة.

إن التعبـير المختصر عن مبرهنـة (٥-١-٥) هو: الامتداد الجبري على الجبري يكون جبريًا.

إن للنتائج السابقة أهمية خاصة في حالة كون F حقل الأعداد النسبية و K حقل الأعداد المركبة.

تعريف:

*يطلق على العدد المركب اسم **عدد جبري** (algebraic number) إذا كان جبريًا على حقل الأعداد النسبية.*

يطلق على العدد المركب الذي ليس جبريًا اسم **عدد متسام** (transcendental number). في هذه المرحلة لا يمكننا الادِّعاء بوجود أعداد متسامية ولكن في البند القادم سنبرهن على أن العدد المألوف e متسام. وهذا سيثبت بالطبع وجود أعداد متسامية. في الحقيقة إن هذه الأعداد كثيرة جدًّا، وبمعنى محدد يوجد منها أكثر من الأعداد الجبرية.

بتطبيق مبرهنة (٥ـ١ـ٤) على حالة الأعداد الجبرية نستنتج أن هذه الأعداد تكون حقلا، أي أن حاصل جمع وضرب وخارج قسمة الأعداد الجبرية هي أعداد جبرية أيضا.

عند استعمال مبرهنة (٥ـ١ـ٥) مع ما يدعى «بمبرهنة الجبر الأساسية» نستنتج أن جذور كثيرة الحدود التي معاملاتها أعداد جبرية هي أعداد جبرية بحد ذاتها.

مسائل

١ - برهن على أن التطبيق $\psi:F[x] \to F(a)$ المعرف وفق القاعدة $h(x)\psi=h(a)$ هو تشاكل.

٢ - ليكن F حقلا و F[x] حلقة كثيرات الحدود في x على F. ولتكن g(x) في F[x] من الدرجة n و $V=(g(x))$ المثالي المولد بواسطة g(x) في F[x]. أثبت أن F[x]/V **فضاء متجهات** بعده يساوي n على الحقل F.

٣ - (ا) إذا كان V فضاء متجهات منته البعد على الحقل K وكان F حقلاً جزئيًا من K بحيث أن [K:F] منته . برهن على أن V فضاء متجهات منته البعد على F وأن

$$\dim_F(V)=(\dim_K(V))([K:F])$$

(ب) بين أن مبرهنة (٥-١-١) هي حالة خاصة من النتيجة في جزء (ا) .

٤ - (ا) ليكن R حقل الأعداد الحقيقية و Q حقل الأعداد النسبية . في R العنصران $\sqrt{2}$ و $\sqrt{3}$ جبريان على Q. اكتب كثيرة حدود من الدرجة الرابعة يحققها العنصر $\sqrt{2}+\sqrt{3}$.

(ب) ما هي درجة $\sqrt{2}+\sqrt{3}$ على Q ؟ برهن على إجابتك .

(جـ) ما هي درجة $\sqrt{2}\sqrt{3}$ على Q ؟

٥ - باستعمال نفس رموز مسألة ٤ . أثبت أن $\sqrt{2}+\sqrt[3]{5}$ جبري على Q من الدرجة السادسة .

*٦ - (أ) أوجد عنصرًا u في R بحيث $Q(\sqrt{2},\sqrt[3]{5})=Q(u)$

(ب) في $Q(\sqrt{2},\sqrt[3]{5})$ ميِّز جميع العناصر w بحيث $Q(w)\neq Q(\sqrt{2},\sqrt[3]{5})$

٧ - (ا) برهن على أن $F(a,b)=F(b,a)$

(ب) إذا كان $(i_1,i_2,\ldots,i_n)$ أي تبديل من $(1,2,\ldots,n)$ فبرهن على أن

$$F(a_1,\ldots,a_n)=F(a_{i_1},a_{i_2},\ldots,a_{i_n})$$

٨ - إذا كان a و b في K جبريين على F من الدرجة m و n على الترتيب وكان m و n أوليين نسبيًا . فبرهن على أن درجة $F(a,b)$ على F تساوي mn.

٩ - لنفرض أن F حقل يحوي عددًا منتهيًا q من العناصر .

(ا) برهن على أنه يوجد عدد أولي p بحيث أن $a+a+\ldots+a$ (p من المرات) لجميع a في F.

(ب) برهن على أن $q=p^n$ لعدد صحيح ما n.

(جـ) إذا كان a في F ، فبرهن على أن $a^q=a$

(د) إذا كان b في K جبريًا على F. فبرهن على أن $b^{q^m}=b$ لعـــدد ما $m>0$.

يقال إن العدد الجبري a **عدد جبري صحيح** (algebraic integer) إذا حقق معادلة من الشكل $a^m+\alpha_1a^{m-1}+\ldots+\alpha_m=0$ حيث $\alpha_1,\ldots,\alpha_m$ أعداد صحيحة .

١٠ ـ إذا كان a أي عدد جبري . فبرهن على أنه يوجد عدد صحيح موجب n بحيث إن na عدد جبري صحيح .

١١ ـ إذا كان العدد النسبي r عددًا جبريًا صحيحًا، فبرهن على أن r يجب أن يكون عددا صحيحا اعتياديا .

١٢ ـ إذا كان a عددًا جبريًا صحيحًا و m عددًا صحيحًا اعتياديًا، فبرهن على :

(ا) أن $a+m$ عدد جبري صحيح .

(ب) ma عدد جبري صحيح .

١٣ ـ إذا كان α عددًا جبريًا صحيحًا يحقق $\alpha^3+\alpha+1=0$ و β عددا جبريا صحيحا يحقق $\beta^2+\beta-3=0$ فبرهن على أن كلا من $\alpha+\beta$ و $\alpha\beta$ عدد جبري صحيح .

١٤** ـ (ا) برهن على أن حاصل جمع عددين جبريين صحيحين هو عدد جبري صحيح .

(ب) برهن على أن حاصل ضرب عددين جبريين صحيحين هو عدد جبري صحيح .

١٥ ـ (ا) برهن على أن $\sin 1^o$ هو عدد جبري .

(ب) من الجزء (ا) برهن على أن $\sin m^o$ هو عدد جبري لأي عدد صحيح m.

(٥ ـ ٢) تسامي العدد e

عندما عرفنا الأعداد الجبرية والمتسامية أشرنا إلى أنه يمكن إثبات وجود **الأعداد المتسامية** (transcendental numbers). إن إحدى الطرق لتحقيق ذلك هي تبيان كون عدد معين متساميا .

في عام ١٨٥١م قدم العالم ليوفيل (Liouville) معيارًا لكون عدد مركب جبريًا وباستعمال هذا المعيار استطاع أن يكتب مجموعة كبيرة من الأعداد المتسامية . على سبيل المثال يُستنتج من عمله أن العدد ...10...101001000000100. متسام حيث عدد الأصفار بين الواحد والذي يليه هو على النمط ...,n!,...,1!,2! إن هذا بالتأكيد يحسم مسألة وجود هذه الأعداد. ومع ذلك فإن السؤال عن كون عدد مألوف ما متسام يبقى قائما. إن أول نجاح في هذا الاتجاه كان على يد العالم هرمايت (Hermite) الذي قدم

في عام **١٨٧٣**م برهانًا بأن e عدد متسام ، ثم بُسِّط برهانه كثيرا بواسطة الرياضي هلبرت (Hilbert) . البرهان الذي سنعرضه هنا يعود إلى هرفتز (Hurwitz) وهو يختلف بعض الشيء عن برهان هلبرت .

إن برهـان كـون العـدد π متساميا أمـر أصعـب من برهـان e. ولكـن لندمـان (lindemann) استطـاع التغلب على الصعـوبات وبرهـن في عـام **١٨٨٢**م على أن π متسـام . وكنتيجـة حتمية من ذلـك هي استحـالـة تربيع الدائرة باستعمال المسطرة والفرجار، لأن مثل هذا البناء سيؤدي إلى عدد جبري θ بحيث $\pi=\theta^2$. ولكن إذا كان θ جبريًّا يكون θ^2 كذلك وعليه يكون π جبريا مما يناقض استنتاج لندمان .

في عام **١٩٣٤**م استـطاع العـالمـان جلفاند (Gelfond) وشنايدر (Schneider) القيام بعملين مستقلين عن بعضهما، إثبات أنه إذا كان a و b عددين جبريين وكان b غير نسبي فإن a^b عدد متسام . إن هذا يجيب بالإيجاب على سؤال هلبرت عن كون $2^{\sqrt{2}}$ عددا متساميا .

للقـراء المهتمـين بمتـابعـة موضوع الأعداد المتسامية ننصحهم بالرجـوع إلى كتـاب سيجـل **(C.L.Siegel)** المفيد وعنوانه **"transcendental Numbers"** أو كتـاب **"Irrational Numbers"** ومـؤلفه نفن **(I.Niven)**

كي نبرهن على أن e **غير نسبي** (irrational) أمر سهل أما برهان كون π غير نسبي فهو أصعب كثيرا . ولكن هناك برهان بسيط نسبيا يمكن للقارىء الاطّلاع عليه بالعودة إلى بحث كتبه نفن (Niven) بعنوان :

Niven, I. "A Simple Proof that π is Irrational". *Bulletin of the American Mathematical Society,* 53(1947), page 509.

الآن لنبرهن على أن e متسام . بالرغم من أن البرهان مهم بحد ذاته فهو أيضا يعتبر تغييراً عمَّا ألفناه من البراهين المقدمة إلى هذا الحد في هذا الكتاب والتي يغلب عليها

الطابع الجبري. أما الآن فنعود ولفترة قصيرة إلى مفاهيم التفاضل والتكامل الأكثر ألفة للقارىء. إن البرهان سيستعمل أفكارا أولية من التفاضل والتكامل، وأعمق نتيجة سنستعملها هي مبرهنة القيمة المتوسطة.

مبرهنة (٥-٢-١)

العدد e متسام

البرهان

في هذا البرهان سنستعمل الرمز المتفق عليه $f^{(i)}(x)$ ليعني المشتقة من الرتبة i لـ f(x) بالنسبة إلى x.

لنفرض أن f(x) كثيرة حدود من الدرجة r ومعاملاتها أعداد حقيقية. وليكن:

$$F(x)=f(x)+f^{(1)}(x)+f^{(2)}(x)+\ldots+f^{(r)}(x)$$

لنحسب $\left(\frac{d}{dx}\right)(e^{-x}F(x))$ باستعمال الحقيقة القائلة إن $f^{(r+1)}(x)=0$ (لأن درجة f(x) تساوي r) وبالاستعانة بخاصة e الأساسية وهي أن $\left(\frac{d}{dx}\right)e^{x}=e^{x}$، نحصل على:

$$\left(\frac{d}{dx}\right)(e^{-x}F(x))=-e^{-x}f(x)$$

إن مبرهنة القيمة المتوسطة تؤكد أنه إذا كانت g(x) دالة مفردة القيمة ذات مشتقة متصلة معرّفة على الفترة المغلقة $[x_1,x_2]$ فإن:

$$\frac{g(x_1)-g(x_2)}{x_1-x_2}=g^{(1)}(x_1+\theta(x_2-x_1))$$

حيث $0<\theta<1$.

نطبق هذا على دالتنا $e^{-x}F(x)$ التي من الواضح أنها تحقق جميع شروط مبرهنة القيمة المتوسطة على الفترة المغلقة $[x_1,x_2]$ حيث $x_1=0$ و $x_2=k$، حيث k أي عدد صحيح موجب. عندئذ نحصل على:

$e^{-k}F(k)-F(0)=-e^{-\theta_k k}(\theta_k k)k$ حيث θ_k يعتمد على k وهو عبارة عن عدد حقيقي بين 0 و 1. عند ضرب هذه العلاقة بـ e^k نحصل على :

$$F(k)-F(0)e^k=-e^{(1-\theta_k)k}f(\theta_k k)k$$

نكتب هذا صريحا كما يلي :

$$F(1)-eF(0)=-e^{(1-\theta_1)}f(\theta_1)=\varepsilon_1,$$

$$F(2)-e^2F(0)=-2e^{2(1-\theta_2)}f(2\theta_2)=\varepsilon_2, \qquad (١)$$

$$\vdots$$

$$F(n)-e^nF(0)=-ne^{(1-\theta_n)}f(n\theta_n)=\varepsilon_n$$

لنفرض الآن أن e عدد جبري . إذن e يحقق علاقة من الصيغة :

$$c_ne^n+c_{n-1}e^{n-1}+\ldots+c_1e+c_0=0$$

حيث $c_0,c_1,\ldots,c_n$ أعداد صحيحة و $c_0>0$ (٢)

في العلاقة (١) لنضرب المعادلة الأولى بـ c_1 والثانية بـ c_2 وهكذا. بجمع هذه المعادلات مع بعضها نحصل على :

$$c_1F(1)+c_2F(2)+\ldots+c_nF(n)-F(0)(c_1e+c_2e^2+\ldots+c_ne^n)=c_1\varepsilon_1+c_2\varepsilon_2+\ldots+c_n\varepsilon_n.$$

وفقا للعلاقة (٢) يكون $c_1e+c_2e^2+\ldots+c_ne^n=-c_0$ لذا فإن المعادلة أعلاه تصبح :

$$c_0F(0)+c_1F(1)+\ldots+c_nF(n)=c_1\varepsilon_1+\ldots+c_n\varepsilon_n \qquad (٣)$$

كل ما عملناه صحيح لأية دالة F[x] منشأه كما في أعلاه من كثيرة حدود اختيارية f(x) نرى ما نحصل عليه عند استعمالنا لكثيرة حدود معينة استعملها لأول مرة هرمايت ، ألا وهي :

$$f(x)=\frac{1}{(p-1)}x^{p-1}(1-x)^p(2-x)^p\ldots(n-x)^p$$

حيث p أي عدد أولي نختاره بحيث $p>n$ و $p>c_0$. لكثيرة الحدود هذه سوف نتفحص جيدا $F(0),F(1),\ldots,F(n)$ وسوف نقدر كذلك مقدار كل من $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n$.

عند نشر $f(x)$ نحصل على كثيرة حدود من الصيغة :

$$\frac{(n!)^p}{(p-1)!}x^{p-1}+\frac{a_0x^p}{(p-1)!}+\frac{a_1x^{p+1}}{(p-1)!}+\ldots,\ .,$$

حيث $a_0,a_1,\ldots$ أعداد صحيحة .

عندما يكون $i\geqslant p$ فإننا ندعي أن $f^{(i)}(x)$ هي كثيرة حدود معاملاتها أعداد صحيحة وهي مضاعفات للعدد p. (برهن على ذلك، انظر مسألة ٢) . *لذا فلكل عدد صحيح j ، $f^{(i)}(j)$ هو عدد صحيح من مضاعفات p إذا كان $i\geqslant p$.*

من تعريف $f(x)$ فإن لها جذر تكراره p عند $x=1,2,\ldots,n$. لذا فلكل $j=1,2,\ldots,n$ ، $f(j)=0$ ، $F^{(1)}(j)=0$ ، ... ، $f^{(p-1)}(j)=0$ وحيث إن $F(j)=f(j)+f^{(1)}(j)+\ldots+f^{(p-1)}(j)+f^{(p)}(j)+\ldots+f^{(r)}(j)$ فوفقا لما قُدِّم أعلاه يكون *$F(j)$ عددا صحيحا من مضاعفات p لكل $j=1,2,\ldots,n$.*

ماذا عن $F(0)$ ؟ لما كان لكثيرة الحدود $f(x)$ جذر تكراره $p-1$ عند $x=0$ ، فإن $f(0)=f^{(1)}(0)=\ldots=f^{(p-2)}(0)=0$. عندما $i\geqslant p$ ، فإن $f^{(i)}(0)$ عدد صحيح من مضاعفات p. ولكن $f^{(p-1)}(0)=(n!)^p$ ولكون $p>n$ وهو عدد أولي، فإن $p\nmid(n!)^p$. لذا فإن $f^{(p-1)}(0)$ هو عدد صحيح *لا يقبل القسمة على p*. وحيث إن :

$$F(0)=f(0)+f^{(1)}(0)+\ldots+f^{(p-2)}(0)+f^{(p-1)}(0)+f^{(p)}(0)+\ldots+f^{(r)}(0)$$

نستنتج أن *$F(0)$ عدد صحيح لا يقبل القسمة على p*. ولما كان $c_0>0$ و $p>c_0$ ولكون $p\nmid F(0)$ بينما $p|F(1),p|F(2),\ldots,p|F(n)$ ، فإن $c_0F(0)+c_1F(1)+\ldots+c_nF(n)$ عدد صحيح *لا يقبل القسمة على p.*

ولكن وفقا لـ (٣) $c_0F(0)+c_1F(1)+ \dots +c_nF(n)=c_1\varepsilon_1+ \dots +c_n\varepsilon_n$ ماذا يمكن القول عن ε_i ؟ لنتذكر أن :

$$\varepsilon_i=\frac{-e^{i(1-\theta_i)}(1-i\theta_i)^p\dots(n-i\theta_i)^p(i\theta_i)^{p-1}i}{(p-1)!},$$

حيث $0<\theta_i<1$. لذا

$$|\varepsilon_i|\leqslant e^n\frac{n^p\,(n!)^p}{(p-1)!}.$$

عندما $p\to\infty$ فإن :

$\frac{e^n n^p(n!)^p}{(p-1)!}\to 0$ (برهن على ذلك) لذا يمكننا إيجاد عدد أولي أكبر من c_0 و n وهو من الكبر بحيث إن : $|c_1\varepsilon_1+\dots+c_n\varepsilon_n|<1$ ولكن $c_1\varepsilon_1+\dots+c_n\varepsilon_n=c_0F(0)+\dots+c_nF(n)$ *مما يجعله عددًا صحيحًا* ولكونه أصغر من 1 نستنتج أن $c_1\varepsilon_1+\dots+c_n\varepsilon_n=0$. ونتيجة لذلك يكون $c_0F(0)+\dots+c_nF(n)=0$. ولكن هذا يناقض كون $p\nmid(c_0F(0)+\dots+c_nF(n))$ بينما $p|0$. إن التناقض الذي حصلنا عليه من فرض كون e جبريا يبرهن على أن العدد يجب أن يكون متساميا .

مســائــل

١ - باستعمال المتسلسلة اللانهائية للعدد e:

$$e=1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}+\dots+\frac{1}{n!}+\dots$$

برهن على أن e عدد غير نسبي .

٢ - إذا كانت $g(x)$ كثيرة حدود معاملاتها أعداد صحيحة ، فبرهن على أنه إذا كان p عددا أوليا فإنه لكل $i\geqslant p$ ،

$$\frac{d^i}{dx^i}\left(\frac{g(x)}{(p-1)!}\right)$$

هي كثيرة حدود معاملاتها أعداد صحيحة كل منها يقبل القسمة على p.

٣ ـ إذا كان a أي عدد حقيقي. فبرهن على أن: $(a^m/m!) \to 0$ عندما $m \to 0$.

٤ ـ إذا كان $m>0$ و n عددين صحيحين. فبرهن على أن العدد $e^{m/n}$ متسام.

(٥ ـ ٣) جذور كثيرات الحدود

في بند (٥ـ١) درسنا عناصر في امتداد ما K لـ F والتي كانت جبرية على F. أي عناصر تحقق كثيرات حدود في F[x]. أما الآن فنعكس المسألة. أي إذا أعطينا كثيرة حدود p(x) في F[x] فإننا نريد إيجاد حقل K امتداد لـ F والذي فيه يوجد جذر لـ p(x). لم يعد الحقل K متوفرًا لدينا، وفي الحقيقة أن هدفنا الرئيس هو إنشاؤه. وعند الانتهاء من إنشائه سوف ندرسه عن كثب ونرى ما هي النتائج التي يمكننا أن نشتقها من ذلك.

تعريف

إذا كان p(x) في F[x] فإن العنصر a الواقع في امتداد ما للحقل F يدعى جذرا (root) لـ p(x) إذا كان $p(a)=0$.

نبدأ بالنتيجة المألوفة والمعروفة باسم **مبرهنة الباقي**.

تمهيدية (٥ ـ٣ ـ١)

إذا كان p(x) في F[x] وكان K امتدادًا لـ F ، فإنه لأي عنصر b في K يكون $p(x)=(x-b)q(x)+p(b)$ حيث q(x) في K[x] وحيث $\deg q(x)=\deg p(x)-1$.

البرهان

لما كان $F\subset K$ فإن $F[x]\subset K[x]$ ، لذا يمكننا أن نعتبر p(x) عنصرًا في K[x].

باستعمال خوارزم التقسيم لكثيرات الحدود في K[x] نحصل على:

$p(x)=(x-b)q(x)+r$ حيث $q(x)$ في $K[x]$ و $r=0$ أو $\deg r<\deg (x-b)=1$.

لـذا فـإن $r=0$ أو $\deg r=0$ وفـي كلتـا الحالتـين يكـون r عنصـرًا فـي K. ولكـن أي عنصـر فـي K هـو؟ لـمـا كـان $p(x)=(x-b)q(x)+r$ فـإن $p(b)=(b-b)q(b)+r=r$. إذن $p(x)=(x-b)q(x)+p(b)$. نترك للقارىء التحقق من أن : $\deg q(x)=\deg p(x)-1$ وهو أمر سهل.

نتيجة

إذا كان a في K جذرًا لـ $p(x)$ في $F[x]$ حيث $F\subset K$ فإن $(x-a)|p(x)$ في $K[x]$.

البرهان

من تمهيدية (٥-٣-١)، $p(x)=(x-a)q(x)+p(a)$ في $K[x]$. ولكن $p(a)=0$. لذا يكون $p(x)=(x-a)q(x)$ وبناءً عليه $(x-a)|p(x)$ في $K[x]$.

تعريف

*يدعى العنصر a في K جذرا **تكراره** (multiplicity) m لـ $p(x)$ في $F[x]$ إذا كان $(x-a)^m|p(x)$ بينما $(x-a)^{m+1}\nmid p(x)$.*

من الأسئلة المعقولة التي يمكن طرحها هنا هو: كم من الجذور يمكن لكثيرة حدود أن تملك في حقل ما؟ قبل أن نجيب على السؤال يجب أن نقرر كيفية احتساب الجذر الذي تكراره m. سوف نحسبه *دائمًا على أنه m من الجذور*. الآن لدينا التمهيدية التالية.

تمهيدية (٥-٣-٢)

لا يمكن أن يكون لكثيرة حدود من الدرجة n على حقل أكثر من n من الجذور في أي امتداد للحقل.

البرهان

سنستعمل الاستقراء الرياضي على n ، درجة كثيرة الحدود p(x). إذا كانت درجة p(x) تساوي 1 ، فيجب أن يكون p(x) على الصيغة $\alpha x+\beta$ حيث α و β في حقل ما F وحيث $\alpha\neq 0$. إذا كان $p(a)=0$ لعنصر ما a فيجب أن يكون $\alpha a+\beta=0$ ونستنتج في هذا أن $a=(-\beta/\alpha)$. أي أن لـ p(x) جذرًا وحيدًا وهو $-\beta/\alpha$ ، لذا فإن التمهيدية صحيحة في هذه الحالة.

لنفرض أن التمهيدية صحيحة لجميع الحقول وجميع كثيرات الحدود من الدرجة m حيث $m<n$ ، ولنفرض أن درجة p(x) على F تساوي n. ليكن K أي امتداد لـ F. إذا لم يكن لـ p(x) جذور في K ، فإن التمهيدية صحيحة لكون عدد الجذور يساوي صفرا وهو أقل من n. لذا نفرض أن لـ p(x) جذرًا واحدًا على الأقل في K وليكن a. ونفرض أن تكراره يساوي m. لما كان $(x-a)^m|p(x)$ فإن $m\leq n$. الآن $p(x)=(x-a)^m q(x)$ حيث q(x) في K[x] من الدرجة n–m. من حقيقة كون $(x-a)^{m+1}\nmid p(x)$ نستنتج أن $(x-a)\nmid q(x)$ وعليه فإن a ليس جذرا لـ q(x) حسب النتيجة لتمهيدية (٥-٣-١). إذا كان b في K جذرا لـ p(x) و $b\neq a$ ، فإن $0=p(b)=(b-a)^m q(b)$ ، ونستنتج من هذا أن $q(b)=0$ ذلك لأن $b-a\neq 0$ ولأننا نعمل داخل حقل. أي أن، أي جذر لـ p(x) في K عدا a يجب أن يكون جذرًا لـ q(x). ولما كانت درجة q(x) هي n–m و $n-m<n$ ، فاستنادا إلى فرضية الاستقراء يكون لـ q(x) جذور في K عددها n–m على الأكثر. وبإضافة الجذر الآخر a والذي نحتسبه m من الجذور، يكون لـ p(x) $m+(n-m)=n$ من الجذور على الأكثر في الحقل K. هذا يكمل الاستقراء وينهي برهان التمهيدية.

يجب التأكيد هنا على أن خاصة الإبدال ضرورية في تمهيدية (٥-٣-٢) إذا اعتبرنا حلقة الرباعيات الحقيقية التي لا يفصل بينها وبين كونها حقلا إلا أنها غير إبدالية. إن لكثير الحدود x^2+1 ثلاثة جذور على الأقل وهي i,j,k (في الحقيقة إن له عددًا غير منتهٍ من الجذور) في حلقة الرباعيات الحقيقية. ومن جانب آخر نؤكد أن خاصة الإبدال وحدها لا تكفي إذ يجب أن تكون الحلقة حلقة تامة. فلو كان $ab=0$ حيث $a\neq 0$ و $b\neq 0$

في الحلقة الإبدالية R ، فإن لكثيرة الحدود ax من الدرجة 1 على R جذرين مختلفين على الأقل هما x=0 و x=b في R.

بالرغم من كون التمهيدتين السابقتين شيقتين ولكنهما ذاتا أهمية ثانوية. الآن نبدأ بإنجاز مهمتنا الرئيسة وهي إنشاء امتداد مناسب لـ F والذي فيه يكون لكثيرة حدود ما جذور. وعندما ننتهي من ذلك، يمكننا دراسة مثل هذه الامتدادات إلى حد معقول وكاف من الدقة لنخرج بنتائج معيّنة. إن أهم خطوة في الإنشاء تنجزها لنا المبرهنة التالية. إن المناقشة الواردة في البرهان ستذكّرنا ببعض ما ذكرناه في بند (٥ ـ ١).

مبرهنة (٥-٣-١)

إذا كانت $p(x)$ كثيرة حدود في $F[x]$ من الدرجة $n\geqq 1$ وهي غير مختزلة على F ، عندئذ يوجد امتداد E لـ F بحيث $[E:F]=n$ ويكون لـ $p(x)$ جذر فيه.

البرهان

لتكن $F[x]$ حلقة كثيرات الحدود في x على F وليكن $V=(p(x))$ المثالي في $F[x]$ والمولد بواسطة $p(x)$. وفقا لتمهيدية (٣-٩-٦) فإن V مثالي أعظمي في $F[x]$. لذا فإن $E=F[x]/V$ حقل استنادا لمبرهنة (٣-٥-١). إننا سنبين أن E هذا يحقق استنتاج المبرهنة.

أولا: نريد أن نبين أن E امتداد لـ F ، بيد أنه في الحقيقة ليس كذلك. ولكن دع $\bar{F}$ يساوي صورة F في E ، أي أن $\bar{F}=\{\alpha+V|\alpha\in F\}$. إننا نزعم أن $\bar{F}$ هو حقل يماثل F وفي الحقيقة إذا كان ψ التطبيق من $F[x]$ إلى $F[x]/V=E$ والمعرّف بواسطة $f(x)\psi=f(x)+V$ ، فإن اقتصار ψ على F يعطينا تماثلا من F على $\bar{F}$ (برهن ذلك!). باستعمال هذا التماثل نطابق F مع $\bar{F}$ ، *وبهذه الطريقة يمكننا اعتبار E امتدادًا لـ F.*

إننا ندعي أن E امتداد منتهٍ لـ F درجته $n=\deg p(x)$ ، ذلك لأن العناصر

$$1+V, x+V, (x+V)^2=x^2+V, \dots, (x+V)^i=x^i+V, \dots, (x+V)^{n-1}=x^{n-1}+V$$

تكون أساسا لـ E على F (برهن على ذلك!) . لغرض تسهيل عملية الترميز دعنا نرمز لـ $x\psi=x+V$ في الحقل E بالرمز a. ونسأل: ما هي قيمة $f(x)\psi$ لعنصر ما $f(x)$ في $F[x]$ ؟ إننا ندعي أنه مجرد $f(a)$ ذلك لأنه إذا كانت $f(x)=\beta_0+\beta_1x+\dots+\beta_kx^k$ فإن $f(x)\psi=\beta_0\psi+(\beta_1\psi)(x\psi)+\dots+(\beta_k\psi)(x\psi)^k$ بسبب كون ψ تشاكلا. وباستعمال التطابق المشار إليه أعلاه لـ $\beta\psi$ مع β نستنتج أن $f(x)\psi=f(a)$. لما كانت $p(x)$ في V فإن $p(x)\psi=0$ ولكن $p(x)\psi=p(a)$ ، إذن $p(a)=0$ ، أي أن العنصر $a=x\psi$ في E هو جذر لـ $p(x)$. بهذا يكون الحقل E متمتعا بجميع الصفات المطلوبة في نص مبرهنة (٥-٣-١) مما ينهي البرهان.

نتيجة

إذا كانت $f(x)$ في $F[x]$ فيوجد امتداد منتهٍ E لـ F يحوي جذرًا لـ $f(x)$. وفضلا عن ذلك $[E:F]\leq\deg f(x)$

البرهان

ليكن $p(x)$ عاملا غير مختزل لـ $f(x)$ ، كل جذر لـ $p(x)$ هو جذر لـ $f(x)$. وفقا للمبرهنة يوجد امتداد E لـ F بحيث: $[E:F]=\deg p(x)\leq\deg f(x)$ وهو يحوي جذرًا لـ $p(x)$ وبالتالي لـ $f(x)$.

إن الحقيقة التالية بالرغم من كونها نتيجة للنتيجة أعلاه ولكن لأهميتها العظمى نكتبها على صيغة مبرهنة.

مبرهنة (٥-٣-٢)

لتكن $f(x)$ في $F[x]$ من الدرجة $n\geq1$. عندئذ يوجد امتداد E لـ F درجته لا تزيد عن $n!$ يحوي n من الجذور لـ $f(x)$ (أي جذورها بأجمعها).

البرهان

في نص المـبرهنـة نعتبر الجذر الذي تكراره m عبارة عن m من الجذور. وفقا للنتيجـة أعـلاه يوجد امتداد E_0 لـ F بحيث $[E_0:F]\leqslant n$ وفيه f(x) تملك جذرا α. لذا تتحلل f(x) إلى $f(x)=(x-\alpha)q(x)$ في الحلقـة $E_0[x]$ حيث درجـة q(x) تسـاوي n−1. باستعمال الاستقراء (أو بتكرار العملية أعلاه) يوجد امتداد E لـ E_0 درجته لا تزيد عن !(n−1) وفيه q(x) يملك n−1 من الجذور. ولما كان أي جذر لـ f(x) هو إما α أو جذر لـ q(x) ، نستنتج أن E يحوي جميع جذور f(x) والتي عددها n. الآن

$$[E:F]=[E:E_0][E_0:F]\leqslant(n-1)!n=n!$$

وهذا ينهي إثبات المبرهنة.

إن مبرهنة (٥-٣-٢) تؤكد وجود امتداد منته E يحوي n من الجذور لكثيرة حدود معـطاة من الـدرجـة n على F. إذا كانت $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ حيث $a_0\neq0$ وإذا كانت جذور f(x) في E هي العناصر $\alpha_1,\ldots,\alpha_n$. فباستعمال النتيجة لتمهيدية (٥-٣-١) يمكننا تحليل f(x) على E بالشكل $f(x)=a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$. لذا فإن f(x) تنشطر تمامًا على E كحاصل ضرب عوامل خطية (من الدرجة الأولى). طالما يوجد امتداد منته لـ F متمتع بهذه الخاصة فإنه يوجد *امتداد منته لـ F ذو درجة دنيا* ويتمتع بالخـاصـة ذاتها أي تفريق f(x) إلى حاصل ضرب عوامل خطية. لمثل هذا الامتداد الأدنى لا يمكن إيجـاد حقـل جزئي فعلي تتحلل فيه f(x) إلى حاصل ضرب عوامل خطية. هذا يدعونا إلى التعريف التالي.

تعريف

إذا كانت *f(x) فـي F[x] ، فنـدعـو أي امتـداد منتـه E لـ F حـقـل انشـطار (splitting field) على F لـ f(x) إذا أمكن تحليل f(x) على E إلى حاصل ضرب عوامل خطية ولكن لا يمكن عمل ذلك على أي حقل جزئي فعلي من E.*

نعـود فنقول إن مبرهنة (٥-٣-٢) تضمن وجود *حقل انشطار*. في الحقيقة إنها تنص على أكثر من ذلك، إذ أنها تؤكد على أنه يوجد لأي كثيرة حدود من الدرجة n على

F حقل انشطار هو امتداد لـ F ودرجته لا تزيد عن !n على F. سوف نرى فيما بعد أنه يمكن التوصل إلى هذا الحد الأعلى !n ، بمعنى أنه إذا أعطينا n فبإمكاننا إيجاد حقل F وكثيرة حدود من الدرجة n في F[x] بحيث أن درجة حقل انشطار f(x) على F تساوي !n.

إن العبارة التالية مكافئة للتعريف الذي قدمناه لحقل انشطار f(x) على F: يدعى الحقل E *حقل انشطار لـ f(x) على F إذا كان E امتدادًا أدنى لـ F والذي يوجد فيه لـ n f(x) من الجذور، حيث n=deg f(x)*. إن السؤال الذي يطرح نفسه هنا هو: إذا كان E_1 و E_2 حقلي انشطار لكثيرة الحدود f(x) في F[x] ، فما هي العلاقة بينهما؟ من نظرة أولى، لا يحق لنا الفرض بوجود أية علاقة بينهما. إن مهمتنا القادمة هي بيان أنهما بالفعل ذوا علاقة وثيقة ببعضهما، والحقيقة أنهما متماثلان بواسطة تماثل يترك كل عنصر في F دون تغيير. الآن نبدأ بالعمل في هذا الاتجاه.

ليكن F و F′ حقلين و τ تماثلا من F على F′. من أجل السهولة نرمز لصورة أي عنصر α في F تحت تأثير τ بالرمز α′ أي α′=ατ. سوف نحتفظ بهذا الترميز في الصفحات القليلة القادمة.

هل يمكننا استعمال τ لتعريف تماثل بين F[x] و F′[t] ؟ نعم. ولنجرب الأمر الواضح وهو إذا كانت $f(x)=\alpha_0x^n+\alpha_1x^{n-1}+\ldots+\alpha_n$ كثيرة حدود اختيارية في F[x] فنعرف *τ وفقا لما يلي:

$$f(x)\tau^*=(\alpha_0x^n+\alpha_1x^{n-1}+\ \ldots\ +\alpha_n)\tau^*=\alpha_0't^n+\alpha_1't^{n-1}+\ \ldots+\alpha_n'.$$

إن برهان التمهيدية التالية بسيط جدا نتركه للقارىء.

تمهيدية (٥-٣-٣)

**τ يعرف تماثلا من F[x] على F′[t] بحيث ατ*=α′ لكل α في F.*

إذا كانت f(x) في F[x] فسوف نكتب f(x)τ* على الشكل f′(t) إن تمهيدية (٥-٣-٣)

تقتضي حتــما أن يُنتج تحليل $f(x)$ في $F[x]$ تحليلاً مشـابهًـا لـ $f'(t)$ في $F'[t]$ والعكس بالعكس. وبصورة خاصة تكون $f(x)$ في $F[x]$ غير مختزلة إذا وفقط إذا كانت $f'(t)$ غير مختزلة في $F'[t]$.

ومع هذا فإن حلقات كثيرات الحدود لا تعنينا في الوقت الحاضر ولكن المهم هو امتـدادات F. دعنا نتذكر أنه في برهاننا لمبرهنة (٥-١-٢) استعملنا الحلقات الخارجة لحلقات كثيرات حدود للحصول على امتدادات مناسبة من F. ونتيجة لذلك يبدو من الـطبيعي أن ندرس العلاقة بين $F[x]/(f(x))$ و $F'[t]/(f'(t))$ حيث $(f(x))$ يرمز للمثالي المـولَّد بواسطة $f(x)$ في $F[x]$ و $(f'(t))$ المثالي المولَّد بواسطة $f'(t)$ في $F'[t]$. إن التمهيدية القادمة ذات صلة وثيقة بهذا الموضوع وهي في الوقت نفسه جزء من نتيجة عامة في نظرية الحلقات ولكننا سنكتفي بتقديمها في الشكل الذي يتلاءم ودراستنا الحالية.

تمهيدية (٥-٣-٤)

يوجـد تـمـاثل τ^{**} من $F[x]/(f(x))$ على $F'[t]/(f'(t))$ بحيث أنه لجميع العناصر α في F يكون $\alpha\tau^{**}=\alpha'$ و $(x+(f(x)))\tau^{**}=t+f'(t)$.

البرهان

قبل البدء بالبرهان يجب أن نوضح المقصود بالجزء الأخير من نص التمهيدية. كـمـا فعلنـا من قبـل ولعـدة مرات، يمكننا اعتبار الحقل F مُدْخلاً في $F[x]/(f(x))$ بمـطابقـة العنصر α في F بالمجمـوعـة المشـاركـة $\alpha+(f(x))$ في $F[x]/(f(x))$. وبصـورة مشابهة يمكننا اعتبار F' محتوى في $F'[t]/(f'(t))$. لذا فإنه يُفترض في التماثل τ^{**} أن يحقق $(\alpha+f(x))\tau^{**}=\alpha'+f'(t)$.

إننا نبحث عن تماثل τ^{**} من $F[x]/(f(x))$ على $F'[t]/(f'(t))$ ولا نجد أسهل من أن نجرب التطبيق τ^{**} المعرَّف وفقا لـ $[g(x)+(f(x))]\tau^{**}=g'(t)+(f'(t))$ لكل $g(x)$ في $F[x]$.

نترك للقارىء تفاصيل التحقق من أن τ^{**} حسن التعريف وأنه تمـاثل من $F[x]/(f(x))$ على $F'[t]/(f'(t))$ يتمتع بجميع الصفات التي تنص عليها تمهيدية (٥-٣-٤).

إن تمهيدية (٥-٣-٤) تمكننـا من تحقيق الخطوة الأولى نحو غايتنا وهي إثبات وحدانية حقول الانشطار، إذ يمكننا الآن برهان ما يلي.

مبرهنة (٥-٣-٣)

إذا كانت $p(x)$ غير مختزلة في $F[x]$ وكان v جذرًا لـ $p(x)$ ، فإن $F(v)$ يماثل $F'(w)$ حيث w جذر لـ $p'(t)$ وبالاضافة إلى ذلك يمكننا اختيار هذا التماثل σ بحيث يكون:

١ - $v\sigma=w$

٢ - $\alpha\sigma=\alpha'$ لكل α في F.

البرهان

ليكن v جذرًا لكثيرة الحدود غير المختزلة $p(x)$ موجودا في امتداد ما K لـ F. ودع

$$M=\{f(x)\in F[x]|f(v)=0\}$$

من الواضح أن M مثالي في $F[x]$ وأن $M\neq F[x]$. وحيث إن $p(x)$ في M وأنها كثيرة حدود غير مختزلة نستنتج أن $M=(p(x))$. كما في برهان المبرهنة (٥-١-٢) نعرف تطبيقا ψ من $F[x]$ إلى $F(v)$ وفقا لـ:

$$q(x)\psi = q(v) \text{ لكل } q(x) \text{ في } F[x]$$

لقد رأينا سابقا (في برهان مبرهنة ٥-١-٢) أن ψ يطبق $F[x]$ على $F(v)$. إن نواة ψ هي بالضبط M أي $(p(x))$. وفقا لمبرهنة التشاكل الأساسية للحلقات يوجد تماثل ψ^* من $F[x]/(p(x))$ على $F(v)$. لاحظ أيضا أن $\alpha\psi^*=\alpha$ لكل α في F. وباختصار التطبيق ψ^* هو تـمـاثل من $F[x]/(p(x))$ على $F(v)$ يترك جميع عناصر F دون تغيير ومن خواصه أن $v=[x+(p(x))]\psi^*$. لما كانت $p(x)$ غير مختزلة في $F[x]$ فإن $p'(t)$ غير مختزلة في $F'[t]$ (وفقا لتمهيدية ٥-٣-٣) وبناءً عليه يوجد تماثل θ^* من $F'[t]/(p'(t))$ على $F'(w)$ حيث w جذر لـ $p'(t)$ بحيث يترك θ^* جميع عناصر F' دون تغيير وأن $w=[t+p'(t)]\theta^*$.

الآن نجمـع الأجزاء مع بعضها كي تثبت مبرهنة (٥-٣-٣). فوفقا لتمهيدية (٥-٣-٤) يوجد تماثل τ^{**} من $F[x]/(p(x))$ على $F'[t]/(p'(t))$ يتوافق مع τ على F ويأخذ $x+(p(x))$ إلى $t+(p'(t))$. لنعتبر التطبيق $\sigma=(\psi^*)^{-1}\tau^{**}\theta^*$ موضحا في الشكل

$$F(v)\xrightarrow{(\psi^*)^{-1}}\frac{F[x]}{(p(x))}\xrightarrow{\tau^{**}}\frac{F[t]}{(p'(t))}\xrightarrow{\theta^*}F'(w)$$

من $F(v)$ على $F'(w)$. إنه تماثل من $F(v)$ على $F'(w)$ لأن كلا من التطبيقات ψ^* ، τ^{**} ، θ^* هو تماثل غامر. لما كان $v=[x+(p(x)]\psi^*$ فإن :

$$v\sigma=(v(\psi^*)^{-1})\tau^{**}\theta^*=([x+(p(x))]\tau^{**})\theta^*=[t+(p'(t))]\theta^*=w.$$

كذلك لكل α في F يكون

$$\alpha\sigma=(\alpha(\psi^*)^{-1})\tau^{**}\theta^*=(\alpha\tau^{**})\theta^*=\alpha'\alpha^*=\alpha'$$

لقد بيّنا أن σ تماثل يحقق جميع الشروط المنصوص عليها في المبرهنة مما يكمل البرهان.

إن حالة خاصة من المبرهنة أعلاه مهمة بحد ذاتها وهي النتيجة التالية.

نتيجة

إذا كانت $p(x)$ في $F[x]$ غير مختزلة وكان a و b جذرين لـ $p(x)$ فإن $F(a)$ يماثل $F(b)$ بتماثل يأخذ a إلى b ويترك جميع عناصر F دون تغيير.

الآن نأتي إلى المبرهنة التي كما ذكرنا من قبل تعتبر حجر الأساس لنظرية جالوا. وهي الغاية الأساسية من هذا البند.

مبرهنة (٥-٣-٤)

أي حقلي انشطار E و E' لكثيرتي الحدود $f(x)$ في $F[x]$ و $f'(t)$ في $F'[t]$ على الترتيب متماثلان بواسطة تماثل ϕ يتمتع بالخاصية $\alpha\phi=\alpha'$ لكل α في F. (بصورة خاصة كل حقلي انشطار لكثيرة حدود ما على أي حقل F متماثلان بواسطة تماثل يترك جميع عناصر F دون تغيير).

البرهان

يبدو من المناسب استعمال طريقة الاستقراء الرياضي في البرهان. ومن أجل ذلك فإننا نحتاج إلى مؤشر قيمه أعداد صحيحة يتناقص باستعمال طريقة ما ضمن خطوات عملنا. إن المؤشر الذي سنستعمله هو درجة حقل انشطار ما على الحقل الابتدائي. قد يبدو لأول وهلة أن اختيارنا هذا مصطنع (وقد يكون مصطنعًا فعلا) ولكننا نفعل ذلك لأنه كما سترى، أن مبرهنة (٥-٣-٣) توفر لنا الطريقة لإنقاص هذا المؤشر.

إذا كان $[E:F]=1$ فإن $E=F$ وعليه فإن $f(x)$ تنشطر إلى حاصل ضرب عوامل خطية على F نفسه. استنادا إلى تمهيدية (٥-٣-٣) فإن $f'(t)$ تنشطر على F' إلى حاصل ضرب عوامل خطية مما يجعل $E'=F'$. ولكن عندئذ يوفر لنا التطبيق $\tau=\phi$ التماثل من E على E' والذي يتفق مع τ على F.

لنفرض أن النتيجة صحيحة لأي حقل F_0 وأي كثيرة حدود $f(x)$ في $F_0[x]$ بحيث أن درجة أحد حقول انشطاره E_0 على F_0 أقل من n. أي أن $[E_0:F_0]<n$.

نفرض أن $[E:F]=n>1$ حيث E حقل انشطار لـ $f(x)$ على F. لما كان $n>1$ فإن لـ $f(x)$ عاملا غير مختزل $p(x)$ درجته $r>1$. ليكن $p'(t)$ العامل غير المختزل المقابل لـ $f'(t)$. لما كان E يشطر $f(x)$ فإن E يحوي جميع جذور $f(x)$ وبالتالي جميع جذور $p(x)$. لذا يوجد عنصر v في E بحيث $p(v)=0$. وفقا لمبرهنة (٥-١-٣) فإن $[F(v):F]=r$. بصورة مشابهة يوجد عنصر w في E' بحيث $p'(w)=0$. استنادا لمبرهنة (٥-٣-٤) يوجد تماثل σ من $F(v)$ على $F'(w)$ يتمتع بالخاصية $\alpha\sigma=\alpha'$ لكل α في F.

لما كان $[F(v):F]=r>1$ ، فإن

$$[E:F(v)]=\frac{[E:F]}{[F(v):F]}=\frac{n}{r}<n$$

إننا ندَّعي أن E حقل انشطار لـ $f(x)$ باعتبارها كثيرة حدود على $F_0=F(v)$. ذلك لأنه لا يوجد حقل جزئي فعلي من E يحوي F_0 وبالتالي F وفي نفس الوقت يشطر $f(x)$ لأننا افترضنا أن E حقـل انشـطار لـ $f(x)$ على F. بصورة مشابهة يكون E' حقل انشطار لـ $f'(t)$ على $F'_0=F'(w)$. باستعـمال فرضية الاستقراء يوجد تماثل ϕ من E على E' بحيث $a\phi=a\sigma$ لكـل a في F_0. ولكن لكـل α في F ، $\alpha\sigma=\alpha'$. إذن لكـل α حيث $\alpha\in F\subset F_0$ ، يكون $\alpha\phi=\alpha\sigma=\alpha'$. هذا ما يكمل الاستقراء ويثبت المبرهنة.

لغرض برهنة الجزء الأخير من نص المبرهنة دع $F=F'$ و τ التطبيق المحايد وهو $\alpha\tau=\alpha$ لكل α في F. لنفرض أن E_1 و E_2 حقلا انشطار لـ $f(x)$ في $F[x]$ ، باعتبار $E_1=E\supset F$ و $E_2=E'\supset F'=F$ نستنتج أن E_1 يماثل E_2 بواسطة تماثل يترك عناصر F دون تغيير وذلك استنادا إلى المبرهنة التي قد انتهينا من إثباتها أعلاه.

بالنظر للحقيقة أن كل حقلي انشطار لكثيرة حدود على F متماثلان بواسطة تماثل يترك جميع عناصر F دون تغيير، يمكننا التحدث عن حقل الانشطار كاسم معرف بدلا من مجرد حقل انشطار ذلك لأنه وحيد بالضرورة.

أمثلـــــــــة

(١) ليكن F حقلا ما و $p(x)=x^2+\alpha x+\beta$ حيث α و β في F. إذا كان K أي امتداد لـ F يحوي جذرًا a لـ $p(x)$ ، فإن العنصر $b=-\alpha-a$ موجود أيضا في K و هو جذر لـ $p(x)$. إذا كان $b=a$ فإنه من السهل التأكد من أن $p(x)=(x-a)^2$ وعليه يقع جذرا $p(x)$ في K. وإذا كان $b\neq a$ ففي هذه الحالة أيضا يكون جذرا $p(x)$ في K. نستنتج من ذلك أنه يمكن شطر $p(x)$ بواسطة امتداد درجته 2 على F. يمكننا التوصل إلى النتيجة نفسها باستخدام مبرهنة (٥-٣-٢) مباشرة.

(٢) ليكن F حقل الأعداد النسبية و $f(x)=x^3-2$. إن جذور $f(x)$ في حقل الأعداد المركبة هي $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.. حيث $\omega=(-1+\sqrt{3}\,i)/2$ و $\sqrt[3]{2}$.. هو الجـذر التكعيبي الحقيقي للعدد 2. إن الحقل $F(\sqrt[3]{2})$ لا يمكن أن يشطر x^3-2 لأنه حقل جزئي من

حقل الأعداد الحقيقية فلا يمكن له أن يحوي $\omega\sqrt[3]{2}$ لأنه عدد مركب غير حقيقي. ماذا يمكننا القول عن E حقل انشطار x^3-2 على F دون تعيينه صراحة؟ وفقا لمبرهنة (٥-٣-٢) نحصل على $[E:F]\leqslant 3!=6$ ، ولما كانت x^3-2 غير مختزلة على F حسب ملاحظتنا أعلاه ولكون $[F(\sqrt[3]{2}):F]=3$ فاستنادا لنتيجة مبرهنة (٥-١-١) نحصل على

$$[E:F]>[F(\sqrt[3]{2}):F]=3 \text{ ولكون } 3=[F(\sqrt[3]{2}):F]\,|\,[E:F].$$

فلا يبقى لنا إلا أن يكون $[E:F]=6$. يمكننا أن نحصل على النتيجة ذاتها بعمل امتدادين هما $F_1=F(\sqrt[3]{2})$ و $E=F_1(\omega)$ وبيان أن ω تحقق كثيرة حدود غير مختزلة من الدرجة الثانية على F_1.

(٣) ليكن F حقل الأعداد النسبية و $f(x)=x^4+x^2+1$ في $F[x]$. إننا ندّعي أن $E=F(\omega)$ حيث $\omega=(1+\sqrt{3}\,i)/2$ هو حقل انشطار لـ $f(x)$. لذا فإن $[E:F]=2$ وهو عدد يقل كثيرًا عن القيمة القصوى وهي $4!=24$.

مسائل

١ - في برهان تمهيدية (٥-٣-١)، أثبت أن $\deg q(x)=\deg p(x)$

٢ - في برهان مبرهنة (٥-٣-١)، أثبت بالتفصيل أن العناصر $1+V, x+V, \ldots, x^{n-1}+V$ تكون أساسا لـ E على F.

٣ - برهن تفصيلا تمهيدية (٥-٣-٣).

٤ - في تمهيدية (٥-٣-٤) بين أن τ^{**} حسن التعريف وهو تماثل من $F[x]/(f(x))$ على $F[t]/(f'(t))$.

٥ - في مثال (٣) في نهاية هذا البند. أثبت أن $F(\omega)$ هو حقل انشطار لـ x^4+x^2+1.

٦ - ليكن F حقل الأعداد النسبية. عين درجة حقول الانشطار لكثيرات الحدود أدناه :

(أ) x^4+1 (ب) x^6+1

(جـ) x^4-2 (د) x^5-1

(هـ) x^6+x^3+1

٧ - ليكن p عددا أوليا. برهن على أن درجة حقل انشطار x^p-1 على حقل الأعداد النسبية تساوي $p-1$.

٨** ـ إذا كان $n>1$. فبرهن على أن درجة حقل انشطار x^n-1 على حقل الأعداد النسبية تساوي $\Phi(n)$ حيث Φ هي دالة أويلر (Euler). إن هذه المسألة هي في الحقيقة مبرهنة معروفة ولا أعرف حلاً بسيطًا لها، لذا فلا تشعر بخيبة أمل إذا عجزت عن حلها. إذا حصلت على حل بسيط فإنني أرغب في الاطلاع عليه. هذه المسألة ستصادفنا بصيغة مكافئة في مسألة (٥ـ١) في بند (٥ـ٦).

٩* ـ إذا كان F حقل الأعداد النسبية. فأوجد الشروط الضرورية والكافية على العنصرين a و b بحيث تكون درجة حقل انشطار x^3+ax+b تساوي 3 على الحقل F.

١٠ ـ ليكن p عددا أوليا و $F=Z_p$ حقل الأعداد الصحيحة قياس p

(ا) برهن على أنه يوجد كثيرة حدود غير مختزلة من الدرجة 2 على F.

(ب) استعمل كثيرة الحدود هذه لبناء حقل يحوي p^2 من العناصر.

(جـ)* أثبت أن أي كثيرتي حدود غير مختزلتين من الدرجة 2 على F تقودانا إلى حقلين متماثلين يحويان p^2 من العناصر.

١١ ـ إذا كان E امتدادًا لـ F و $f(x)$ في $F[x]$ وإذا كان ϕ تماثلا ذاتيًا للحقل E يترك جميع عناصر F دون تغيير. فبرهن على أن ϕ يجب أن يأخذ جذرًا لـ $f(x)$ موجودًا في E إلى جذر لـ $f(x)$ في E.

١٢ ـ أثبت أنه لا يوجد تماثل ذاتي للحقل $F(\sqrt[3]{2})$ حيث F حقل الأعداد النسبية عدا التماثل الذاتي المحايد.

١٣ ـ باستعمال نتيجة مسألة (١١) برهن على أنه إذا كان العدد المركب α جذرًا لكثيرة الحدود $p(x)$ التي *معاملاتها أعداد* حقيقية، فإن $\bar{\alpha}$.. هو جذر أيضا لـ $p(x)$ حيث $\bar{\alpha}$.. العدد المركب المرافق لـ α.

١٤ ـ باستعمال نتيجة مسألة (١١) برهن على أنه إذا كان m عددًا صحيحًا لا يساوي مربع عدد صحيح آخر وكان $\alpha+\beta\sqrt{m}$ (حيث α ، β أعداد نسبية) جذرًا لكثيرة الحدود $p(x)$ التي *معاملاتها أعداد* نسبية فإن $\alpha-\beta\sqrt{m}$ هو أيضا جذر لـ $p(x)$.

١٥* ـ إذا كان F حقل الأعداد الحقيقية. فبرهن على أنه إذا كان ϕ تماثلا ذاتيا لـ F فإن ϕ يترك جميع عناصر F ثابتة.

١٦ - (ا) أوجد جميع الرباعيات الحقيقية $t=a_0+a_1i+a_2j+a_3k$ التي تحقق $t^2=-1$.

(ب)• إذا كان t كما في جزء (ا). فبرهن على أنه يوجد رباعي حقيقي s بحيث أن $sts^{-1}=i$.

(٥ - ٤) الإنشاء الهندسي باستعمال المسطرة والفرجار

نتوقف في هذا البند عن تطوير دراستنا العامة لنتفحص بعض ما تقتضيه النتائج التي حصلنا عليها حتى الآن في مواضع هندسية مألوفة.

يدعى العدد الحقيقي α عددا *قابلا للإنشاء* (constructible) إذا أمكننا إنشاء قطعة مستقيم طولها α باستخدام المسطرة والفرجار فقط. نفرض أن لدينا وحدة قياس طول أساسية. ولنتذكر أنه في دراستنا للهندسة في المدرسة الثانوية تمكّنا من إنشاء مستقيم عمودي ومستقيم مواز لمستقيم معلوم يمر بنقطة معيّنة وذلك باستخدام المسطرة والفرجار فقط. من هذا نجد أنه من السهل البرهان على أنه إذا كان α و β عددين قابلين للإنشاء فإن الأعداد $\alpha\pm\beta$ ، $\alpha\beta$ و α/β عندما $\beta\neq0$ كلها قابلة للإنشاء (انظر مسألة ١). لذا نستنتج أن مجموعة الأعداد القابلة للإنشاء تكون حقلاً جزئيًا W من حقل الأعداد الحقيقية.

على وجه الخصوص ولكون $1\in W$ فإن W يجب أن يحوي F_0 حقل الأعداد النسبية. إننا نود دراسة علاقة W بحقل الأعداد النسبية.

وحيث إننا سنصادف التعبير «الإنشاء باستعمال المسطرة والفرجار» (واشتقاقات أخرى منه) *فإن الكلمات: أنشىء، قابل للانشاء وإنشاء كلها تعني استعمال المسطرة والفرجار.*

إذا كان $w\in W$ فبإمكاننا التوصل إلى w بَدْءًا بحقل الأعداد النسبية باستخدام عدد منتهٍ من الانشاءات.

ليكن F أي حقل جزئي من حقل الأعداد الحقيقية . لنعتبر جميع النقط (x,y) في المستوى الإقليدي الحقيقي التي إحداثياها x و y يقعان في F. نطلق على مجموعة هذه النقط مستوى F. إن كل مستقيم يصل بين نقطتين في مستوى F له معادلة على الشكل $ax+by+c=0$ حيث a ، b و c عناصر في F (انظر مسألة ٢) . بالإضافة إلى ذلك أية دائرة يكون مركزها في مستوى F وطول نصف قطرها عنصر في F لها معادلة على الشكل $x^2+y^2+ax+by+c=0$ حيث a ، b و c في F (انـظر مسـألـة ٣). نصف مثـل هذه المستقيمات والدوائر بأنها *مستقيمات ودوائر في F*.

إذا تقاطـع مستقيمـان في F في نقطـة على المستوى الحقيـقي فإن هذه النقطة تقع في مستوى F (انظر مسألة ٤) . من جهة أخرى ليس من الضروري أن تقع نقطة تقاطـع مستقـيم في F مع دائرة في F في مستـوى F. ولكن باستخدام حقيقة أن معادلة مستقـيم في F هي على الشكـل $ax+by+c=0$ ومعــادلــة دائـرة في F على الشكـل $x^2+y^2+dx+ey+f=0$ حيث a ، b ، c ، d ، e ، f عناصر في F يمكننا أن نبيّن أنه إذا تقاطع في المستوى الحقيقي مستقيم في F مع دائرة في F فإما أن تقع نقطة تقاطعهما في مستوى F أو في مستوى $F(\sqrt{\gamma})$ حيث γ عـدد موجـب في F (انظر مسألة ٥) . وأخـيرا فإن تقـاطـع دائـرتـين في F يمكن أن يعتـبر كتقاطع لمستقـيم في F مع دائـرة في F فلو كانت هاتـان الدائرتـان هما $x^2+y^2+a_1x+b_1y+c_1=0$ و $x^2+y^2+a_2x+b_2y+c_2=0$ فإن تقاطعهما هو تقاطع أيٍّ منهما مع المستقيم $(a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0$ والذي يعطينا نقطة إما في مستوى F أو مستوى $F(\sqrt{\gamma})$ حيث γ عدد موجب في F.

لـذا فإن المستقيمات والدوائر في F تقودنا إلى نقط إما في F أو في امتداد تربيعي من F. إذا اعتبرنا أننا في $F(\sqrt{\gamma_1})$ وهو امتداد تربيعي ما من F فإن المستقيمات والدوائر في $F(\sqrt{\gamma_1})$ تقـاطـع في نقط تقـع في مستوى $F(\sqrt{\gamma_1},\sqrt{\gamma_2})$ حيث γ_2 عدد موجب في $F(\sqrt{\gamma_1})$. نصف نقــطة بأنها قابلة للإنشــاء من F إذا أمكننـا إيجـاد أعـداد حقيقية $\lambda_1,\ldots,\lambda_n$ بحيث $\lambda_1^2\in F$ ، $\lambda_2^2\in F(\lambda_1)$ ، $\lambda_3^2\in F(\lambda_1,\lambda_2)$ ، $\lambda_n^2\in F(\lambda_1,\ldots,\lambda_{n-1})$. وحـيث إن النقطة تقع في مستوى $F(\lambda_1,\ldots,\lambda_n)$. وبالعكس إذا كان γ في F بحيث $\sqrt{\gamma}$ عدد حقيقي

فيمكن أن يدرك $\sqrt{\gamma}$ على أنه ناتج من تقاطع مستقيمات ودوائر في F (انظر مسألة ٦). لذا تكون النقطة قابلة للإنشاء من F إذا وفقط إذا أمكننا إيجاد عدد منته $\lambda_1,\ldots,\lambda_n$ من الأعداد الحقيقية بحيث:

١ - $[F(\lambda_1):F]=1,2$

٢ - $[F(\lambda_1,\ldots,\lambda_i):F(\lambda_1,\ldots,\lambda_{i-1})]=1,2$

لكل $i=1,2,\ldots,n$ وبشرط أن النقطة تقع في مستوى $F(\lambda_1,\ldots,\lambda_n)$.

لقد سبق وأن عرّفنا العدد الحقيقي القابل للإنشاء α إذا أمكننا باستعمال المسطرة والفرجار إنشاء قطعة مستقيم طولها α. ولكن هذا يصبح بدلالة المناقشة أعلاه كالتالي: يكون العدد α قابلاً للإنشاء إذا تمكننا بدءًا بمستوى الأعداد النسبية F_0 إدخال α في حقل يمكن الحصول عليه من F_0 بواسطة عدد منتهٍ من الامتدادات التربيعية. أي تصبح لدينا المبرهنة التالية.

مبرهنة (٥-٤-١)

يكون العدد الحقيقي α قابلًا للإنشاء إذا وفقط إذا أمكننا إيجاد عدد منته من الأعداد الحقيقية $\lambda_1,\ldots,\lambda_n$ بحيث

١ - λ_1^2 *في* F_0 ،

٢ - λ_i^2 *في* $F_0(\lambda_1,\ldots,\lambda_{i-1})$ *لكل* $i=2,3,\ldots,n$. *بحيث* α *في* $F_0(\lambda_1,\ldots,\lambda_n)$.

يمكننا حساب درجة $F_0(\lambda_1,\ldots,\lambda_n)$ على F_0 باستعمال مبرهنة (٥-١-١)

$$[F_0(\lambda_1, \ldots, \lambda_n):F_0]=[F_0(\lambda_1,\ldots,\lambda_n):F_0(\lambda_1, \ldots,\lambda_{n-1})]\ldots$$
$$\times[F_0(\lambda_1,\ldots,\lambda_i):F_0(\lambda_1,\ldots,\lambda_{i-1})]\ldots$$
$$\times[F_0(\lambda_1):F_0]$$

ولما كان كل حد في حاصل الضرب هو إما 1 أو 2 نحصل على أن:

$$[F_0(\lambda_1,\ldots,\lambda_n):F_0]=2^r$$

وتكون لدينا النتيجة التالية.

نتيجة (١)

إذا كان α قابلًا للإنشاء فإنه يقع في امتداد ما من الأعداد النسبية درجته إحدى قوى العدد 2.

إذا كان α قابلًا للإنشاء فوفقا للنتيجة (١) أعلاه يوجد حقل جزئي K من حقل الأعـداد الحقيقية بحيث $\alpha \in K$ و $[K:F_0]=2^r$. ولكن $F_0(\alpha)\subset K$ لذا فبـاستعـمال نتيجة مبرهنة (٥ـ١ـ١) يكون

$$[F_0(\alpha):F_0] | [K:F_0]=2^r$$

مما يجعل $[F_0(\alpha):F_0]$ يساوي إحدى قوى العدد 2. وحيث إنه إذا حقق α كثيرة حدود غير مختزلة من الدرجة k على F_0 يكون $[F_0(\alpha):F_0]=k$ حسب مبرهنة (٥ـ١ـ٣). لذا نحصل على معيار مهم لعدم القابلية على الإنشاء، وهو النتيجة التالية.

نتيجة (٢)

إذا حقق العدد الحقيقي α كثيرة حدود غير مختزلة من الدرجة k على حقل الأعداد النسبية ولم يكن k يساوي إحدى قوى العدد 2 ، فإن α غير قابل للانشاء.

إن هذه النتيجـة أعلاه تمكننا من حل مسألة قديمة وهي عملية تثليث زاوية باستعمال المسطرة والفرجار حيث يمكننا برهان ما يلي.

مبرهنة (٥ـ٤ـ٢)

من المستحيل تثليث الزاوية $60°$ باستعمال المسطرة والفرجار فقط.

البرهان

لـو كـان بإمكاننا تثليث الزاوية $60°$ باستعمال المسطرة والفرجار فإن الطول $\alpha=\cos 20°$ يصبـح قابـلا للإنشـاء. في هذا المـوقف نعـود بذاكـرتنـا إلى المتـطابقـة $\cos(3\theta)=4\cos^3(\theta)-3\cos(\theta)$. بالـتـعـويـض عـن θ بالـزاويـة $20°$ وتـذَكُّـر أن

$\cos 60° = \frac{1}{2}$ ، نحصل على $4\alpha^3 - 3\alpha = \frac{1}{2}$ أي أن $8\alpha^3 - 6\alpha - 1 = 0$. لذا فإن α جذر لكثيرة الحدود $8x^3 - 6x - 1$ على الأعداد النسبية. ولكن كثيرة الحدود هذه غير مختزلة على حقل الأعداد النسبية (انظر مسألة ٧(أ)) ولكون درجته تساوي 3 وهو ليس إحدى قوى العدد 2 نستنتج أن α غير قابل للإنشاء حسب النتيجة (٢) من مبرهنة (٥-٤-١). لذا لا يمكن تثليث الزاوية $60°$ باستعمال المسطرة والفرجار فقط.

هناك مسألة قديمة أخرى وهي مسألة مضاعفة المكعب أي عملية إنشاء مكعب حجمه يساوي ضعف حجم مكعب معطى. إذا كان حجم المكعب الأصلي هو وحدة حجم واحدة فهذا يلزمنا بإنشاء طول α بحيث $\alpha^3 = 2$. ولما كانت كثيرة الحدود $x^3 - 2$ غير مختزلة على الأعداد النسبية (مسألة ٧(ب)) فوفقا للنتيجة (٢) من مبرهنة (٥-٤-١) يكون α غير قابل للإنشاء. وبذا نحصل على المبرهنة التالية.

مبرهنة (٥-٤-٣)

من المستحيل مضاعفة مكعب باستعمال المسطرة والفرجار فقط.

نود الآن أن نعرض شكلا هندسيا آخر لا يمكن إنشاؤه باستعمال المسطرة والفرجار ألا وهو المسبع المنتظم. من أجل تنفيذ مثل هذا الإنشاء يتحتم علينا إنشاء $\alpha = 2\cos(2\pi/7)$. ولكننا ندّعي أن α يحقق $x^3 + x^2 - 2x - 1$ (مسألة ٨) وكثيرة الحدود هذه غير مختزلة على حقل الأعداد النسبية (مسألة ٧(جـ)). نستنتج باستعمال نتيجة (٢) من مبرهنة (٥-٤-١) ما يلي.

مبرهنة (٥-٤-٤)

من المستحيل إنشاء مسبع منتظم (regular septagon) باستعمال المسطرة والفرجار فقط.

مســائــل

١ - برهن على أنه إذا كان α ، β قابلين للإنشاء فكذلك $\alpha\pm\beta$ ، $\alpha\beta$ و α/β (عندما $\beta\neq0$).

٢ - أثبت أن كل خط مستقيم في F له معادلة على الصيغة $ax+by+c=0$ حيث a ، b ، c في F.

٣ - أثبت أن كل دائرة في F لها معادلة على الصيغة $x^2+y^2+ax+by+c=0$ حيث a ، b ، c في F.

٤ - برهن على أنـه إذا تقـاطـع مستقيهان في F في نقطة على المستوى الحقيقي فإنهما يتقاطعان في مستوى F.

٥ - برهن على أنه إذا تقاطع مستقيم في F مع دائرة في F في نقطة على المستوى الحقيقي فإما أن تقع هذه النقطة في مستوى F أو في مستوى $F(\sqrt{\gamma})$ حيث γ عدد موجب في F.

٦ - إذا كان γ في F عددًا موجبًا . فبرهن على أنه يمكن إدراك $\sqrt{\gamma}$ من تقاطع مستقيمات ودوائر في F.

٧ - أثبت أن كثيرات الحدود أدناه غير مختزلة على حقل الأعداد النسبية :

(أ) $8x^3-6x-1$

(ب) x^3-2

(جـ) x^3+x^2-2x-1

٨ - أثبت أن $2\cos(2\pi/7)$ يحقق x^3+x^2-2x-1

(إرشاد = استخدم $2\cos(2\pi/7)=e^{2\pi i/7}+e^{-2\pi i/7}$) .

٩ - أثبت أن **المخمس المنتظم** (regular pentagon) قابل للإنشاء .

١٠ - أثبت أن **المسدس المنتظم** (regular hexagon) قابل للإنشاء .

١١ - أثبت أن **المضلع المنتظم ذا الخمسة عشر ضلعا** (regular 15-gon) قابل للإنشاء .

١٢ - برهن على أنه من الممكن تثليث الزاوية $72°$.

١٣ - أثبت أن **المتسع المنتظم** (regular 9-gon) غير قابل للإنشاء .

١٤*- برهن على أن **المضلع المنتظم ذا السبعة عشر ضلعا** (regular 17-gon) قابل للانشاء .

(٥ ـ ٥) المزيد عن الجذور

نعـود الآن إلى عرضنـا العـام. ليكن F حقلاً ما و F[x] حلقة كثيرات الحدود في x على F.

تعريف

إذا كانت $f(x)=\alpha_0 x^n+\alpha_1 x^{n-i}+\ldots+\alpha_i x^{n-1}+\ldots+\alpha_{n-1}x+\alpha_n$ في F[x] فإن مشتقة f(x) derivative والتي نرمز لها بـ f′(x) هي كثيرة الحدود $f'(x)=n\alpha_0 x^{n-1}+(n-1)\alpha_1 x^{n-2}+\ldots+(n-i)\alpha_i x^{n-i-1}+\ldots+\alpha_{n-1}$ في F(x).

إننا لا نحتاج إلى مفهوم النهايات لغرض تقديم مثل التعريف أعلاه أو لإثبات الخـواص الأسـاسية الشكلية لمشتقـات كثـيرات الحدود. ومع ذلك فلكون F حقلا اختياريا يمكن أن نتوقع حدوث بعض الأمور الغريبة.

في نهاية بند (٥ـ٢) عرفنا المقصود بمميز الحقل. لنستذكر هذا الآن: يقال عن حقـل F إنـه صفـري المميز إذا كان $ma\neq 0$ لكـل $a\neq 0$ في F وكـل عدد صحيح $m>0$. إذا كان $ma=0$ لعـدد صحيح ما $m>0$ ولعنصر $a\neq 0$ في F قيل عن F إنه منته المميز. في هذه الحالة الأخيرة يُعرَّف مميز الحقل F بأنه أصغر عدد صحيح موجب p بحيث $pa=0$ لكل a في F. في الحقيقة إنه إذا كان F منته المميز فإن مميزه p يجب أن يكون عددًا أوليًّا.

نعود الآن إلى مسألة المشتقة وليكن F حقلا مميزه $p\neq 0$. في هذه الحالة تكون مشتقة كثيرة الحدود x^p هي كثيرة الحدود $px^{p-1}=0$. لذا فإن النتيجة المعتادة في حساب التفاضل والتكامل القائلة بأنه إذا كانت مشتقة كثيرة حدود تساوي صفرا فإنه يجب أن يكون ثابتا. (هذه النتيجة لم تعد صحيحة دائما). ولكن إذا كان مميز F يساوي صفرا وكان $f'(x)=0$ حيث f′(x) في F[x] فيجب أن يكون $f(x)=\alpha$ حيث α في F (انظر مسألة ١). في حالة كون مميز الحقل مساويًا لـ p و $p\neq 0$ فيبقى في استطاعتنا وصف كثيرات الحدود

التي مشتقاتها تساوي صفرا وهي على وجه التحديد كثيرات حدود في المتغير x^p (انظر مسألة ٢). الآن نبرهن ما يقابل القواعد الشكلية للتفاضل والتي نعرفها جيدا.

تمهيدية (٥-٥-١)

لكل $f(x)$ و $g(x)$ في $F[x]$ وكل α في F نحصل على ما يلي:

١ - $(f(x)+g(x))'=f'(x)+g'(x)$

٢ - $(\alpha f(x))'=\alpha f'(x)$

٣ - $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$

البرهان

إن برهـان القـاعـدتـين ١ و ٢ سهـل جـدا ونـتركـه للقـارىء. كي نـبرهن القـاعـدة التاليـة لاحظ أنه يكفيـنا برهانها في الحالـة الخاصـة جدا عندما $f(x)=x^i$ و $g(x)=x^j$ حيث i و j عددان صحيحـان موجبـان. ولكن حينئذ $f(x)g(x)=x^{i+j}$ مما يجعل $(f(x)g(x))'=(i+j)x^{i+j-1}$ بيـد أن $f'(x)g(x)=ix^{i-1}x^j=ix^{i+j-1}$ و $f(x)g'(x)=jx^ix^{j-1}$. ونتيجة لذلك يكون $f'(x)g(x)+f(x)g'(x)=(i+j)x^{i+j-1}=(f(x)g(x))'$

تذكر من مبادىء حساب التفاضل والتكامل أنه إذا كان لدالة جذر مكرر في نقطة معيّنة فإن هذا يكافىء تلاشي كل من الدالة ومشتقتها عند تلك النقطة. في وضعنا الحالي حيث F حقل اختياري تبقى هذه العلاقة المتبادلة صحيحة.

تمهيدية (٥-٥-٢)

يكون لكثيرة الحدود $f(x)$ في $F[x]$ جذرًا مكررًا إذا وفقط إذا كان لـ $f(x)$ و $f'(x)$ عامل مشترك غير تافه (أي درجته موجبة).

البرهان

قبل برهان التمهيدية لابد من ذكر الملاحظة التالية: إذا كان لـ $f(x)$ و $g(x)$ في $F[x]$ عامل مشترك غير تافه في $K[x]$ حيث K امتداد لـ F فإن لهما عاملاً مشتركًا غير تافه

في $F[x]$. ذلك لأنه لو كانت $f(x)$ و $g(x)$ أوليتين نسبيا في $F[x]$ لأمكننا إيجاد كثيرتي حدود $a(x)$ و $b(x)$ في $F[x]$ بحيث $a(x)f(x)+b(x)g(x)=1$. وحيث إن هذه العلاقة تبقى صحيحة عندما ننظر للعناصر على أنها في $K[x]$ نستنتج أن $f(x)$ و $g(x)$ أوليتان نسبيًا في $K[x]$ مما يبرهن العبارة أعلاه.

الآن نبدأ ببرهان التمهيدية. من الملاحظة أعلاه يمكننا الفرض دون المساس بعمومية البرهان، إن جميع جذور $f(x)$ تقع في F (وإلا فمد F إلى K حقل انشطار $f(x)$).
إذا كان α جذرًا مكررًا لـ $f(x)$ فإن $f(x)=(x-\alpha)^m q(x)$ حيث $m>1$.
ولكن $((x-\alpha)^m)'=m(x-\alpha)^{m-1}$ حيث يمكن التأكد من ذلك بسهولة، وعليه استنادا لتمهيدية (٥-٥-١) يكون:

$$f'(x)=(x-\alpha)^m q'(x)+m(x-\alpha)^{m-1}q(x)=(x-\alpha)r(x),$$

لأن $m>1$. من هذا نرى أن لـ $f(x)$ و $f'(x)$ عاملاً مشتركًا هو $x-\alpha$ مما يبرهن اتجاهًا واحدًا في التمهيدية.

في الاتجاه الآخر، لو فرضنا أن $f(x)$ لا تملك جذرًا مكررًا، فإن $f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ حيث α_i's $(1\leqslant i\leqslant n)$ كلها مختلفة عن بعضها (إننا نفترض أن $f(x)$ واحدية). ولكن حينئذ:

$$f'(x)=\sum_{i=1}^{n}(x-\alpha_1)\ldots\widehat{(x-\alpha_i)}\ldots(x-\alpha_n)$$

حيث إن العلامة $\wedge$ تعني أن الحد محذوف. إننا ندعي أنه لا يوجد جذر مشترك بين $f(x)$ و $f'(x)$ لأن $f'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)\neq 0$ بسبب كون الجذور كلها مختلفة عن بعضها. ولكن إذا كان لـ $f(x)$ و $f'(x)$ عامل مشترك غير تافه فيجب أن يكون لهما جذر مشترك وهو أي جذر من هذا العامل المشترك. نخرج من هذا بأنه لا يمكن لـ $f(x)$ و $f'(x)$ أن يكون لهما جذر مشترك مما يبرهن الاتجاه الآخر في التمهيدية.

نتيجة (١)

إذا كانت $f(x)$ غير مختزلة في $F[x]$، فإنه:

١ ـ *لا توجد جذور مكررة لـ $f(x)$ إذا كان مميز F يساوي صفرا .*
٢ ـ *إذا كان مميز F يساوي $p\neq 0$ وكان لـ $f(x)$ جذر مكرر،* فيجب أن تكون $f(x)$ على *الهيئة $f(x)=g(x^p)$*

البرهان

لما كانت $f(x)$ غير مختـزلـة فإن عامليهـا الـوحيدين في $F[x]$ هما 1 و $f(x)$. وفقًا للتمهيدية أعلاه إذا كان لـ $f(x)$ جذر مكرر، فيجب أن يكون لـ $f(x)$ و $f'(x)$ عامل مشترك غير تافه مما يؤدي إلى أن $f(x)|f'(x)$. ولكن درجة $f'(x)$ أقل من درجة $f(x)$ لذا لا يوجد مخرج من ذلك إلا أن تكون $f'(x)=0$. عندما يكون مميز F يساوي صفرا فيجب أن تكون $f(x)$ مساويا لثابت ، وبذلك لا يكون لها جذور . أما في حالة كون مميز F يساوي $p\neq 0$ فيجب أن تكون $f(x)=g(x^p)$.

سيكـون لنا عودة لمناقشة ما تقتضيه النتيجة (١) بصورة مفصّلة . ولكن الآن نبرهن نتيجة خاصة سنستعين بها في الفصل السابع عندما نعالج الحقول المنتهية .

نتيجة (٢)

إذا كان F حقلا مميزه $p\neq 0$ فإن لكثيرة الحدود $x^{p^n}-x$ في $F[x]$ جذورا مختلفة ، حيث *$n\geq 1$.*

البرهان

إن مشتقة $x^{p^n}-x$ هي $p^n x^{p^n-1}-1=-1$ لأن مميز F يساوي p. إذن $x^{p^n}-x$ ومشتقتها أوليتان نسبيًا وهذا يقتضي أن $x^{p^n}-x$ ليس لها جذور مكررة حسب التمهيدية .

إن النتيجة (١) لا تلغي إمكانية وجود جذور مكررة لكثيرة حدود غير مختزلة على حقـل مميزة $p\neq 0$. كي نوضـح الأمور نعرض مثالا يكون فيه ما ذكرناه ممكنا . ليكن F_0 حقلا مميزه يساوي 2 و $F=F_0(x)$ حقل الدوال النسبية في x على F_0. إننا ندعي أن كثيرة

الحدود t^2-x في $F[t]$ لا مختزلة على F ومع ذلك فإن جذريها متساويان. كي نبرهن على أنها غير مختزلة يجب أن نبين أنه لا توجد دالة نسبية في $F_0(x)$ مربعها يساوي x والذي هو محتوى مسألة (٤). كي ترى أن لـ t^2-x جذرًا مكررًا لاحظ أن مشتقتها (المشتقة بالنسبة لـ t. لكون x ثابتًا لأنه في F) تساوي $2t=0$. بطبيعة الحال يمكن تقديم أمثلة مشابهة في حالة كون مميز الحقل أي عدد أولي.

لقد أصبحت، الآن، الإمكانية حقيقة. إنها تشير إلى الفرق الكبير الموجود بين حالة المميز 0 وحالة المميز p. إن وجود كثيرات حدود غير مختزلة ذات جذور مكررة في حالة المميز p تقودنا للعناية بدقائق أمور شيقة وفي الوقت نفسه معقدة. إن هذه الأمور تتطلب معالجة متطورة وتفصيلية، لذا فإننا نفضل تجنبها في مرحلة دراستنا هذه. وعليه فإننا نفرض أن جميع الحقول التي سنتطرق لها ضمن شرحنا في كل ما تبقى من هذا الفصل هي حقول صفرية المميز.

تعريف

*يدعى امتداد K لـ F **بأنه امتداد بسيط** (simple extension) من F إذا كان $K=F(\alpha)$ حيث α عنصر ما في K.*

في حالة كون المميز يساوي صفرا (أو تحت شروط معيّنة بالنسبة للامتدادات في حالة المميز $p\neq 0$. انظر مسألة ١٤) يمكن إثبات أن جميع الامتدادات المنتهية هي بالأحرى امتدادات بسيطة. هذا هو فحوى المبرهنة التالية.

مبرهنة (٥-٥-١)

إذا كان F حقلا مميزه يساوي صفرا وكان a ، b جبريين على F فإنه يوجد عنصر c في $F(a,b)$ بحيث $F(a,b)=F(c)$.

البرهان

لتكن $f(x)$ و $g(x)$ كثيرتي الحدود وغير المختزلتين من الدرجة m و n على الترتيب واللتان تتحققان بواسطة a و b على الترتيب. ليكن K امتدادًا لـ F وفيه تنشطر كل من

$f(x)$ و $g(x)$ تمامًا. لما كان مميز F يساوي صفرا فإن جميع جذور $f(x)$ مختلفة وكذلك الحالة بالنسبة لـ $g(x)$. لتكن $a=a_1,a_2,\ldots,a_m$ جميع جذور $f(x)$ و $b=b_1,b_2,\ldots,b_n$ جميع جذور $g(x)$. إذا كان $j\neq 1$ فإن $b_j\neq b_1=b$ وعليه فإن للمعادلة $a_i+\lambda b_j=a_1+\lambda b_1=a+\lambda b$ حل واحد λ في K وهو

$$\lambda=\frac{a_i-a}{b-b_j}$$

لما كان مميز F يساوي صفرا فيجب أن يحوي F عددا غير منتهٍ من العناصر. لذا يمكننا إيجاد عنصر γ في F بحيث $a_i+\gamma b_j\neq a+\gamma b$ لكل i وكل $j\neq 1$. دع $c=a+\gamma b$ إننا ندعي أن $F(c)=F(a,b)$. لما كان $c\in F(a,b)$ فإن $F(c)\subset F(a,b)$. الآن سنبيـن أن كلا من a و b عنصران في $F(c)$ مما يجعل $F(a,b)\subset F(c)$. الآن b يحقق كثيرة الحدود $g(x)$ على F وبالتالي فهو يحقق كثيرة الحدود ذاتها باعتبارها على $K=F(c)$. وإضافة إلى ذلك، إذا كان $h(x)=f(c-\gamma x)$ فإن $h(x)\in K[x]$ و $h(b)=f(c-\gamma b)=f(a)=0$ لأن $a=c-\gamma b$. لذا فإنـه في امتداد ما لـ K يكون لـ $h(x)$ و $g(x)$ عامل مشترك هو $x-b$. إننا ندعي أن $x-b$ هو في الحقيقة القاسم المشترك الأعظم لهما. فلو كان $b_j\neq b$ جذرًا آخر لـ $g(x)$ فإن $h(b_j)=f(c-\gamma b_j)\neq 0$. لأنه حسب اختيارنا لـ γ لا يمكن لـ $c-\gamma b_j$ ، $j\neq 1$ أن يساوي a_i أحد جذور $f(x)$. كذلك لاحظ أن $(x-b)^2\nmid g(x)$ وعليه فإن $(x-b)^2$ لا يمكن أن يقسم القاسم المشترك الأعظم لكل من $h(x)$ و $g(x)$. لذا نستنتج أن $x-b$ هو القاسم المشترك الأعظم لكل من $h(x)$ و $g(x)$ على امتداد ما لـ K. ولكن حينئذ يكون لهما قاسم مشترك أعظم غير تافه على K يقسم $x-b$. ولكون درجة $x-b$ تساوي 1. نستنتج أن القاسم المشترك الأعظم لـ $g(x)$ و $h(x)$ في $K[x]$ هو بالضبط $x-b$. أي أن $x-b$ في $K[x]$ مما يجعل b في K. ولكن $K=F(c)$ فنجد أن $b\in F(c)$. ولكون $a=c-\gamma b$ و b ، c في $F(c)$ و $\gamma\in F\subset F(c)$ نستنتج أن a في $F(c)$ وعليه يكون $F(a,b)\subset F(c)$. من علاقتي الاحتواء المتعاكستين يكون لدينا $F(a,b)=F(c)$.

باستعمال الاستقراء الرياضي يمكننا توسيع النتيجة من عنصرين إلى أي عدد منته من العناصر، أي إذا كانت العناصر $\alpha_1,\ldots,\alpha_n$ جبرية على F فإنه يوجد عنصر c في $F(\alpha_1,\ldots,\alpha_n)$ بحيث $F(c)=F(\alpha_1,\ldots,\alpha_n)$. أي يكون لدينا النتيجة التالية.

نتيجة

يكون كل امتداد منته لحقل مميزه صفرا امتدادًا بسيطًا.

مسـائـل

١ - إذا كان F حقلا مميزه يساوي صفرا و $f(x)$ في $F[x]$ بحيث $f'(x)=0$. فبرهن على أن $f(x)=\alpha$ حيث α في F.

٢ - إذا كان F حقلا مميزه $p\neq 0$ و $f(x)$ في $F[x]$ بحيث $f'(x)=0$. فبرهن على أن $f(x)=g(x^p)$ حيث $g(x)$ في $F[x]$.

٣ - برهن على أن $(f(x)+g(x))'=f'(x)+g'(x)$ و $(\alpha f(x))'=\alpha f'(x)$ لكل $f(x)$ ، $g(x)$ في $F[x]$ و α في F.

٤ - أثبت أنه لا توجد دالة نسبية في $F(x)$ مربعها يساوي x.

٥ - أكمل الاستقراء اللازم لإثبات نتيجة مبرهنة (٥-٥-١).

يقال عن عنصر a في امتداد ما K لـ F إنه **قابل للانفصال** (separable) على F إذا حقق كثيرة حدود على F ليس لها جذور مكررة. يوصف امتداد K لـ F بأنه **قابل للانفصال** على F إذا كانت جميع عناصره قابلة للانفصال على F. يقال عن حقل F إنه **كامل** (perfect) إذا كانت جميع الامتدادات المنتهية منه قابلة للانفصال.

٦ - أثبت أن أي حقل صفري المميز يجب أن يكون حقلاً كاملاً.

٧ - (ا) إذا كان مميز F هو $p\neq 0$. فأثبت أنه لكل a و b في F يكون $(a+b)^{p^m}=a^{p^m}+b^{p^m}$

(ب) إذا كان مميز F هو $p\neq 0$ و K امتدادا من F وكان $T=\{a\in K|a^{p^n}\in F,\ \text{n لعدد ما}\}$ فبرهن على أن T حقل جزئي من K.

٨ - إذا كان K ، T ، و F كما في مسألة ٧(ا). فبين أن كل تماثل ذاتي لـ K والذي يترك جميع عناصر F ثابتة، يجب أن يترك جميع عناصر T ثابتة.

٩* - أثبت أن الحقل F الذي مميزه $p\neq 0$ هو حقل كامل إذا وفقط إذا أمكن إيجاد لكل عنصر a في F عنصر b في F بحيث $b^p=a$.

١٠ - باستخدام نتيجة مسألة ٩. برهن على أن كل حقل منتهٍ هو حقل كامل.

١١** - إذا كان K امتدادا لـ F. فبرهن على أن مجموعة عناصر K القابلة للانفصال على F تكون حقلا جزئيًا من K.

١٢ - إذا كان مميز F هو $p\neq 0$ و K امتدادًا منتهيًا من F. فبرهن على أنه لكل a في K إما أن يكون a^{p^n} في F لعدد ما n أو يمكن إيجاد عدد صحيح m بحيث $a^{p^m}\notin F$ ولكنه قابل للانفصال على F.

١٣ - إذا كان K و F كما في مسألة (١٢) وكان كل عنصر في K وليس في F غير قابل للانفصال على F. فبرهن على أنه لكل a يوجد عدد صحيح n يعتمد على a بحيث إن a^{p^n} يقع في F.

١٤ - إذا كان K امتدادًا منتهيًا لـ F قابلاً للانفصال عليه. فبرهن على أن K امتداد بسيط لـ F.

١٥ - إذا كان أحد العنصرين a أو b قابلا للانفصال على F. فبرهن على أن F(a,b) امتداد بسيط لـ F.

(٥ - ٦) مبادىء نظرية جالوا (Galois)

إذا أعـطينا كثيرة حدود p(x) في حلقة كثيرات الحدود F[x] في المجهول x على الحقل F فسوف نقرن بـ p(x) زمرة تدعي **زمرة جالوا** (Galois group) لكثيرة الحدود p(x). هناك علاقة وثيقة بين جذور كثيرة حدود وزمرة جالوا لها. وفي الحقيقة إن زمرة جالوا ستكون عبارة عن زمرة تبديلات معيّنة لجذور كثيرة الحدود. في هذا البند والبند القادم سنقوم بدراسة هذه الأفكار.

إن طريقة تقديم زمرة جالوا ستكون من خلال حقل انشطار كثيرة الحدود p(x) على F. وعلى وجه التحديد فإن زمرة جالوا لـ p(x) هي عبارة عن زمرة عناصرها تماثلات ذاتية لحقـل انشـطار p(x). وفي الحقيقة إن هذا هو سبب اهتمامنا بالتماثلات الذاتية للحقل في العديد مما سيأتي من مبرهنات. إن المبرهنة الأساسية لنظرية جالوا (مبرهنة ٥-٦-٦) تبـين تقـابـلاً بين الـزمـر الجـزئية لزمـرة جالـوا والحقـول الجـزئية لحقـل الانشطار. من هذا سنستنتج في النهاية شرطا لقابلية الحل **باستخلاص الجذور** (solva-bility by radicals) لمعرفة جذور كثيرة حدود ما وذلك بدلالة البناء الجبري لزمرة جالوا له. من هذا نحصل على النتيجة التقليدية للعالم ابل (Abel) بأن كثيرة الحدود العامة من الـدرجـة الخـامسة غير قابلة للحل باستخلاص الجذور. وفي أثناء دراستنا هذه

سنحصل على مبرهنات شيّقة بحد ذاتها كنتائج جانبية. إحدى هذه المبرهنات هي المبرهنة الأساسية للدوال المتناظرة. إن طريقة معالجتنا للموضوع ستكون على نمط الرياضي ارتن (Artin).

لنستعيد ذاكرتنا بأننا نتعامل مع حقول مميزها يساوي صفرا، وبناءً على ذلك يمكننا الاستعانة بمبرهنة (٥-٥-١) ونتيجتها.

ليكن K حقلاً ما و σ تطبيقًا من K على نفسه. يسمى التطبيق σ **تماثلا ذاتيا** (automorphism) للحقل K إذا كان $\sigma(ab)=\sigma(a)\sigma(b), \sigma(a+b)=\sigma(a)+\sigma(b)$ لكل a و b في K. يقال عن تماثلين ذاتيين σ و τ للحقل K إنهما مختلفان إذا كان $\sigma(a)\neq\tau(a)$ لعنصر ما a في K.

الآن نبدأ دراستنا بما يلي.

مبرهنة (٥-٦-١)

ليكن K حقلا و $\sigma_1,\ldots,\sigma_n$ تماثلات ذاتية مختلفة للحقل K. إذا كانت $a_1,\ldots,a_n$ في K بحيث $a_1\sigma_1(u)+a_2\sigma_2(u)+\ldots a_n\sigma_n(u)=0$ لكل u في K، فإن $a_1=a_2=\ldots a_n=0$.

البرهان

لنفرض أنه بإمكاننا إيجاد مجموعة من العناصر $a_1,\ldots,a_n$ ليست جميعًا مساوية للصفر في K بحيث:

$$a_1\sigma_1(u)+a_2\sigma_2(u)+\ldots+a_n\sigma_n(u)=0$$

لكل u في K. عندئذ من الممكن إيجاد مثل هذه العلاقة بحيث يكون عدد الحدود غير الصفرية أصغر ما يمكن. بإعادة الترقيم يمكننا الفرض أن العلاقة الدنيا هي على الصيغة

$$a_1\sigma_1(u)+\ldots+a_m\sigma_m(u)=0 \qquad (١)$$

حيث إن جميع العناصر $a_1,\ldots,a_m$ مختلفة عن الصفر.

إذا كان $m=1$ فإن $a_1\sigma_1(u)=0$ لكـل u في K ، مما يجعـل $a_1=0$. وهذا مناقض للفرض. لذا يمكننا الفرض أن $m>1$. لما كانت التماثلات مختلفة، فإنه يوجد عنصر c في K بحيث $\sigma_1(c)\neq\sigma_m(c)$. ولما كان cu في K لكل u في K فإن العلاقة (١) تبقى صحيحة في حالة العناصر التي على الشكل cu ، أي

$$a_1\sigma_1(cu)+a_2\sigma_2(cu)+\ldots+a_n\sigma_n(cu)=0$$

لكل u في K. باستخدام الفرضية بأن $\sigma_1,\ldots,\sigma_m$ تماثلات لـ K نحصل على العلاقة :

$$a_1\sigma_1(c)\sigma_1(u)+a_2\sigma_2(c)\sigma_2(u)+\ \ldots\ +a_m\sigma_m(c)\sigma_m(u)=0 \qquad (٢)$$

بضرب العلاقة (١) بـ $\sigma_1(c)$ ثم طرحها من (٢) نحصل على

$$a_2(\sigma_2(c)-\sigma_1(c))\sigma_2(u)+\ldots+a_m(\sigma_m(c)-\sigma_1(c))\sigma_m(u)=0 \qquad (٣)$$

إذا جعلنا $b_i=a_i(\sigma_i(c)-\sigma_1(c))$ لكل $i=2,\ldots,m$ فإن b_i في K و $b_m=a_m(\sigma_m(c)-\sigma_1(c))\neq0$ لأن $a_m\neq0$ و $\sigma_m(c)-\sigma_1(c)\neq0$. ومع ذلك $b_2\sigma_2(u)+\ldots+b_m\sigma_m(u)=0$ لكـــل u في K. إن هذه العملية أعطتنا علاقة أقصر من العلاقة الدنيا (١) وهذا تناقض يثبت صحة المبرهنة.

تعريف

إذا كانت G زمرة تماثلات ذاتية للحقل K ، فإن الحقل المثَّبت (fixed field) من قِبَل الزمرة G هو مجموعة كل العناصر a في K بحيث $\sigma(a)=a$ لكل σ في G.

لاحظ أن التعـريف أعـلاه يبقى صحيحا حتى لو كانت G مجرد مجموعة من التماثلات الذاتية للحقل K. بيد أن الحقل المثبت من قبل مجموعة من التماثلات الذاتية يساوي الحقل المثبت من قبل الزمرة المولّدة من هذه المجموعة (في زمرة التماثلات الذاتية للحقل K) (انظر مسألة ١). لذلك فإننا لا نخسر شيئا حين نعرف هذا المفهوم لزمر التماثلات الذاتية فقط. وعلاوة على ذلك، فإننا سوف نهتم فقط بالحقول المثبتة من قبل زمر تماثلات ذاتية.

في التعـريف أعلاه أطلقنا اسم الحقل المثبت من قبل الزمرة G على مجموعة جزئية من K. ومن أجل أن تكون تسميتنا صحيحة يجدر بنا أن نبرهن التمهيدية التالية.

تمهيدية (٥-٦-١)

إن الحقل المثبَّت من قِبَل الزمرة G هو حقل جزئي من K.

البرهان

ليكن a و b عنصرين في الحقل المثبَّت من قِبَل G. لذا يكون $\sigma(a)=a$ و $\sigma(b)=b$ لكل σ في G. ولكن عندئذ يكون

$$\sigma(a\pm b)=\sigma(a)\pm\sigma(b)=a\pm b \text{ و } \sigma(ab)=\sigma(a)\sigma(b)=ab$$

وبناءً على ذلك يقع $a\pm b$ و ab في الحقل المثبَّت من قِبَل G. إذا كان $b\neq 0$ ، فإن $\sigma(b^{-1})=\sigma(b)^{-1}=b^{-1}$ وعليه يكون b^{-1} في الحقل المثبَّت من قِبَل الزمرة G. بهذا نكون قد تحققنا من أن الحقل المثبَّت من قِبَل G هو حقا حقل جزئي من K.

فيما سيأتي سنُعنى بالتماثلات الذاتية للحقل والتي تؤثر بطريقة محددة على حقل جزئي معيّن.

تعريف

ليكن K حقلًا ما و F حقلًا جزئيًا من K. إن زمرة التماثلات الذاتية لـ K نسبة لـ F والتي نرمز لها بالرمز $G(K,F)$ ، هي مجموعة جميع التماثلات الذاتية لـ K والتي تترك كل عنصر من F ثابتا. أي أن التماثل الذاتي σ للحقل K يقع في $G(K,F)$ إذا وفقط إذا كان $\sigma(\alpha)=\alpha$ لكل α في F.

في الحقيقة إنه من الواضح والهين برهان ما يلي فيما يخص هذه التماثلات.

تمهيدية (٥-٦-٢)

إن $G(K,F)$ هي زمرة جزئية من زمرة التماثلات الذاتية لـ K.

نترك برهان هذه التمهيدية للقارىء. وثمة ملاحظة نذكرها هنا وهي أن الحقل K يجب أن يحوي حقل الأعداد النسبية F_0 ، لأن مميز K يساوي صفرا، وعليه

فيكــون من السهل أن نرى أن الحقل المثبَّت من قِبَل أية زمرة من التماثلات الذاتية لـ K يجب أن يحوي F_0. وعليه فإن أي عدد نسبي يُترك دون تغيير تحت تأثير أي تماثل ذاتي لـ K.

الآن نتوقف كي نفحص بعض الأمثلة على المفاهيم التي قُدّمت أعلاه.

مثال (٥-٦-١)

ليكن K حقل الأعداد المركبة و F حقل الأعداد الحقيقية. لنحسب الزمرة $G(K,F)$. إذا كان σ أي تماثل ذاتي لـ K ولما كان $i^2=-1$ فإن $(\sigma(i))^2=\sigma(i^2)=\sigma(-1)=-1$ وعليه $\sigma(i)=\pm i$. إذا كان σ يترك كل عدد حقيقي دون تغيير فإنه لكل $a+ib$ حيث a و b عددان حقيقيان يكون $\sigma(a+bi)=\sigma(a)+\sigma(b)\sigma(i)=a\pm bi$. إن كلا الاحتمالين، أي كون $\sigma_1(a+ib)=a+ib$ و $\sigma_2(a+ib)=a-ib$ يعرف تماثلا ذاتيا لـ K حيث إن σ_1 هو التماثل الذاتي المحايد و σ_2 يرسل كل عدد مركب إلى مرافقه. لذا فإن $G(K,F)$ هي زمرة رتبتها تساوي 2.

تُرى ما هو الحقل المثبت من قِبل $G(K,F)$ ؟ من المؤكد أنه يحوي F ، ولكن هل يحوي شيئا آخر؟ إذا كان $a+ib$ في الحقل المثبت من قِبل $G(K,F)$ فإن: $a+ib=\sigma_2(a+ib)=a-ib$ مما يجعل $b=0$ و $a=a+ib\in F$ وعليه نرى أن الحقل المثبت لـ $G(K,F)$ هو بالتحديد F نفسه.

مثال (٥-٦-٢)

ليكن F_0 حقل الأعداد النسبية و $K=F_0(\sqrt[3]{2})$ حيث $\sqrt[3]{2}$.. هو الجذر التكعيبي الحقيقي للعــدد 2. إن كل عنصر في K هو على الصيغـة $\alpha_0+\alpha_1\sqrt[3]{2}+\alpha_2(\sqrt[3]{2})^2$ حيث $\alpha_0,\alpha_1,\alpha_2$ أعداد نسبية. إذا كان σ تماثلا ذاتيا لـ K فإن: $(\sigma(\sqrt[3]{2}))^3=\sigma((\sqrt[3]{2})^3)$ ، وعليه يجب أن يكــون $\sigma(\sqrt[3]{2})$ جذرا تكعيبيا للعدد 2 واقعا في K. ولكن هناك جذر تكعيبي حقيقي واحد للعدد 2 ، ولكون K حقلاً جزئيًا من حقل الأعداد الحقيقية، يجب أن يكون $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$. ولكن حينئذ يكون

$$\sigma(\alpha_0+\alpha_1\sqrt[3]{2}+\alpha_2(\sqrt[3]{2})^2)=\alpha_0+\alpha_1\sqrt[3]{2}+\alpha_2\sqrt[3]{2}$$

أي أن σ هو التماثل الذاتي المحايد للحقل K. لذا نرى أن $G(K,F_0)$ يحوي فقط على التطبيق المحايد، وفي هذه الحالة *لا يكون الحقل المثبت من قِبل $G(K,F_0)$ هو F_0 بل هو أكبر من ذلك. إنه الحقل K بأكمله*.

مثال (٥-٦-٣)

ليكن F_0 حقل الأعداد النسبية و $\omega=e^{2\pi i/5}$ ، عندئذ $\omega^5=1$ و ω تحقق كثيرة الحدود $x^4+x^3+x^2+x+1=0$ على F_0. باستخدام معيار ايزنشتاين يمكننا أن نثبت أن $x^4+x^3+x^2+x+1$ غير مختزلة على F_0 (انظر مسألة ٣). لذا فإن درجة $K=F_0(\omega)$ تساوي 4 على الحقل F_0. وكل عنصر في K هو على الصيغة $\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3$ حيث $\alpha_0,\alpha_1,\alpha_2,\alpha_3$ في F_0. الآن، كل تماثل ذاتي σ لـ K يحقق $\sigma(\omega)\neq 1$ لأن $\sigma(1)=1$ ، و $(\sigma(\omega))^5=\sigma(\omega^5)=\sigma(1)=1$ مما يجعل $\sigma(\omega)$ جذرا خامسا للواحد أيضا. ونتيجة لذلك يجب أن يكون $\sigma(\omega)$ أحد الأعداد $\omega,\omega^2,\omega^3,\omega^4$. إننا ندعي أن كلا من هذه الاحتمالات يمكن أن تحدث، ولأجل ذلك دعنا نعرف التطبيقات الأربعة $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ وفقا لـ

$$\sigma_i(\alpha_0+\alpha_1\omega+\alpha_2\omega^2+\alpha_3\omega^3)=\alpha_0+\alpha_1(\omega^i)+\alpha_2(\omega^i)^2+\alpha_3(\omega^i)^3$$

لكل $i=1,2,3,4$. كل واحد من هذه التطبيقات يعرف تماثلا ذاتيا لـ K (انظر مسألة ٤).

إذن، لما كان σ في $G(K,F_0)$ يحدد تماما بواسطة $\sigma(w)$ فإن رتبة الزمرة $G(K,F_0)$ تساوي 4 و σ_1 عنصرها المحايد. في ضوء العلاقات $\sigma_2^2=\sigma_4$ ، $\sigma_2^3=\sigma_3$ ، $\sigma_2^4=\sigma_1$ ، نستنتج أن $G(K,F_0)$ زمرة دورية من الرتبة 4. يمكن البرهان بسهولة على أن الحقل المثبت من قِبل $G(K,F_0)$ هو F_0 نفسه (انظر مسألة ٥). إن الحقل المثبت من قِبل الزمرة الجزئية $A=\{\sigma,\sigma_4\}$ هو مجموعة العناصر التي على الصيغة $\alpha_0+\alpha_2(\omega^2+\omega^3)$ ، وهذا الحقل هو امتداد من F_0 درجته تساوي 2.

بالرغم من كون الأمثلة أعلاه توضيحية غير أنها حالات خاصة جدا، إذ أن $G(K,F)$ في أي منها كانت زمرة دورية. إن هذا لا يمثل نموذجا للحالة العامة إطلاقا، فيمكن لـ $G(K,F)$ أن تكون حتى غير إبدالية (انظر مبرهنة ٥-٦-٣). ولكن رغم كون تلك الأمثلة خاصة فإنها تسلط الضوء على بعض الأمور المهمة.

أولهــا: إنها تبين أهمية دراسة تأثير التماثل الذاتي على جذور كثيرات الحدود،
وثانيها: إن الحقل F *قد لا يساوي* كل الحقل المثبت من قِبل الزمرة G(K,F).
إن الحالات التي يكون فيها الحقل المثبت من قِبل G(K,F) هو بالضبط F نفسه هي الحالات المنشودة وهي التي سنبذل في دراستها بعض الوقت والجهد.

الآن نحسب حدًّا مهمًّا لرتبة الزمرة G(K,F).

مبرهنة (٥-٦-٢)

إذا كان K امتدادا منتهيا لـ F ، فإن G(K,F) زمرة منتهية ورتبتها O(G(K,F)) تحقق $O(G(K,F))\leqslant[K:F]$

البرهان

ليكن $[K:F]=n$ وليكن $u_1,\ldots,u_n$ أساسا لـ K على F. في الزمرة G(K,F) نفرض أنه بإمكـانـنـا إيجاد n+1 من التماثلات الذاتية المختلفة وهي $\sigma_1,\sigma_2,\ldots,\sigma_{n+1}$. وفقا لنتيجة مبرهنة (٤-٣-٣) فإن النظام التالي للمعادلات الخطية المتجانسة في n+1 من المجاهيل $x_1,\ldots,x_{n+1}$:

$$\begin{gathered}\sigma_1(u_1)\,x_1+\sigma_2(u_1)x_2+\ldots+\sigma_{n+1}(u_1)x_{n+1}=0\\ \vdots\\ \sigma_1(u_i)\,x_1+\sigma_2(u_i)x_2+\ldots+\sigma_{n+1}(u_i)x_{n+1}=0\\ \vdots\\ \sigma_1(u_n)\,x_1+\sigma_2(u_n)x_2+\ldots+\sigma_{n+1}(u_n)x_{n+1}=0\end{gathered}$$

له حل غير تافــه (ليست جميع قيم x_i تســاوي صفــرا) وليكن $x_1=a_1,\ldots,x_{n+1}=a_{n+1}$ في K. لذا نحصل على

$$a_1\sigma_1(u_i)+a_2\sigma_2(u_i)+\ldots+a_{n+1}\sigma_{n+1}(u_i)=0 \qquad (١)$$

لكل $i=1,2,\ldots,n$.

لما كانت جميع عنـاصر F تبقى دون تغيير تحت تأثير كل σ_i ولكون أي عنصر اختياري t من K هو على الصيغة $t=\alpha_1u_1+\ldots+\alpha_nu_n$ حيث $\alpha_1,\ldots,\alpha_n$ في F. فإنــه من نظام المعادلات (١) نحصل على

$$a_1\sigma_1(t)+\ldots+a_{n+1}\sigma_{n+1}(t)=0$$

لكل t في K. ولكن هذا يناقض نتيجة مبرهنة (٥-٦-١) مما يثبت مبرهنة (٥-٦-٢).

إن مبرهنة (٥-٦-٣) ذات أهمية بالغة في نظرية جالوا، ولكن بجانب دورها الرئيس هناك، فإنها تساهم في برهان نتيجة تقليدية متعلقة بالدوال النسبية المتناظرة. وإن هذه النتيجة في الدوال المتناظرة، بدورها تلعب دورًا مهمًّا في نظرية جالوا.

أولا: نبدي بعض الملاحظات حول حقل الدوال النسبية في n من المتغيرات على حقل F. لنتذكر أننا عرفنا في بند (٣-١١) حلقة كثيرات الحدود في n من المتغيرات $x_1,\ldots,x_n$ على الحقل F ومنها عرّفنا حقل الدوال النسبية في $x_1,\ldots,x_n$ على F بأنه حلقة خوارج القسمة لمثل كثيرات الحدود هذه. رمزنا لهذا الحقل حينئذ بـ $F(x_1,\ldots,x_n)$.

لتكن S_n زمرة التناظر من الدرجة n باعتبارها تؤثر على المجموعة $\{1,2,\ldots,n\}$. لعنصر σ في S_n وعدد صحيح i حيث $1\leq i\leq n$ لتكن $\sigma(i)$ صورة i تحت تأثير σ. نجعل S_n تؤثر على $F(x_1,\ldots,x_n)$ بالطريقة الطبيعية التالية: لكل σ في S_n و $r(x_1,\ldots,x_n)$ في $F(x_1,\ldots,x_n)$، عرِّف التطبيق الذي يأخذ $r(x_1,\ldots,x_n)$ إلى $r(x_{\sigma(1)},\ldots,x_{\sigma(n)})$. سوف نرمز لهذا التطبيق من $F(x_1,\ldots,x_n)$ على نفسه بالرمز σ أيضا. من الواضح أن هذه التطبيقات تعرف تماثلات ذاتية للحقل $F(x_1\ldots x_n)$. ما هو الحقل المثبَّت في الحقل $F(x_1,\ldots x_n)$ من قِبل S_n؟ إنه يحوي جميع الدوال النسبية $r(x_1,\ldots x_n)$ بحيث $r(x_1,\ldots,x_n)=r(x_{\sigma(1)},\ldots x_{\sigma(n)})$ لكل σ في S_n. ولكن هذه بالذات عناصر $F(x_1,\ldots x_n)$ المعروفة باسم **الدوال النسبية المتناظرة** (symmetric rational functions) وحيث إن هذه الدوال تكوِّن الحقل المثبَّت بواسطة S_n، فإنها تكون حقلاً جزئيًّا من $F(x_1,\ldots x_n)$ يسمى حقل الدوال النسبية المتناظرة والذي نرمز له بالرمز S. فيما سيأتي سنهتم بالأسئلة الثلاث التالية:

١ - ما هي $[F(x_1,\ldots,x_n):S]$؟

٢ - ما هي $G(F(x_1,\ldots,x_n),S)$؟

٣ ـ هل من الممكن وصف S بدلالة أحد الامتدادات السهلة من F ؟
سوف نجيب على هذه الأسئلة الثلاث في وقت واحد.

الآن نقدم بعض الدوال البسيطة من S والتي يمكن إنشاؤها من $x_1,\ldots x_n$. تُعرف هذه الدوال باسم **الدوال المتناظرة الابتدائية** (elementary symmetric functions) في $x_1,\ldots x_n$ ونعرِّفها كما يلي :

$$a_1=x_1+x_2+\ldots+x_n=\sum_{i=1}^{n}x_i,$$

$$a_2=\sum_{i<j}x_ix_j,$$

$$a_3=\sum_{i<j<k}x_ix_jx_k,$$

$$a_n=x_1x_2\ldots x_n.$$

يُتْرَك للقارىء التحقق من أن هذه الدوال دوال متناظرة. في حالة $n=2,3,4$ نكتب هذه الدوال تفصيلا كما يلي :

عندما $n=2$ فإن

$$a_1=x_1+x_2\ ,\ a_2=x_1x_2$$

عندما $n=3$ فإن

$$a_1=x_1+x_2+x_3,$$

$$a_2=x_1x_2+x_1x_3+x_2x_3,$$

$$a_3=x_1x_2x_3,$$

عند ما $n=4$ فإن

$$a_1=x_1+x_2+x_3+x_4,$$

$$a_2=x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4,$$

$$a_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4,$$

$$a_4=x_1x_2x_3x_4.$$

لاحظ أنه عندما $n=2$ فإن x_1 و x_2 هما جذرا كثيرة الحدود $t^2-a_1t+a_2$ ، وعندما $n=3$ فإن x_1,x_2,x_3 هي جذور كثيرة الحدود $t^3-a_1t^2+a_2t-a_3$ ، وعندما $n=4$ فإن x_1,x_2,x_3,x_4 هي جذور كثيرة الحدود $t^4-a_1t^3+a_2t^2-a_3t+a_4$.

لما كانت جميع الدوال $a_1,\ldots,a_n$ واقعة في S ، فإن الحقل $F(a_1,\ldots,a_n)$ والذي نحصل عليه بضم $a_1,\ldots,a_n$ إلى F يجب أن يقع في S. إن غايتنا هي برهان التالي:

١ - $[F(x_1,\ldots,x_n):S]=n!$

٢ - $S=F(a_1,\ldots,a_n)$

لما كانت الزمرة S_n هي زمرة التماثلات الذاتية للحقل $F(x_1,\ldots,x_n)$ التي تترك S دون تغيير، فإن $S_n\subset(F(x_1\ldots x_n),S)$. لذا فباستعمال مبرهنة (٥-٦-٢) يكون

$$[F(x_1,\ldots x_n):S]\geqslant 0(G(F(x_1,\ldots x_n),S))\geqslant 0(S_n)=n!$$

إذا استطعنا أن نبين أن $[F(x_1,\ldots,x_n):F(a_1,\ldots,a_n)]\leqslant n!$ ، فعندئذ وبسبب كون $F(a_1,\ldots,a_n)$ حقلاً جزئيًا من S ، نحصل على

$$n!\geqslant[F(x_1,\ldots x_n):F(a_1,\ldots,a_n)]=[F(x_1,\ldots,x_n):S][S:F(a_1,\ldots,a_n)]\geqslant n!$$

وحينئذ يكون $[F(x_1,\ldots,x_n):S]=n!$ و $[S:F(a_1,\ldots,a_n)]=1$ مما يجعل $S=F(a_1,\ldots,a_n)$ و $S_n=G(F(x_1,\ldots,x_n),S)$ (إن المتساوية الأخيرة هي استنتاج من الجملة الثانية في هذه الفقرة). إن هذه هي بالضبط الاستنتاجات التي ننشدها. لذا فيبقى علينا أن نبرهن على أن

$$[F(x_1,\ldots x_n):F(a_1,\ldots a_n)]\leqslant n!$$

ومن هذا لاحظ أن كثيرة الحدود

$$p(t)=t^n-a_1t^{n-1}+a_2t^{n-2}+\ldots+(-1)^na_n$$

والتي معاملاتها في $F(a_1,\ldots,a_n)$ تتحلل على $F(x_1,\ldots,x_n)$ على النحو $p(t)=(t-x_1)(t-x_2)\ldots(t-x_n)$ (في الحقيقة، هذا هو أصل الدوال المتناظرة الابتدائية). لذا فإن $p(t)$ التي درجتها n على $F(a_1,\ldots,a_n)$ تنشطر إلى حاصل ضرب عوامل خطية على الحقل $F(x_1,\ldots x_n)$. ولا يمكنها أن تنشطر على حقل جزئي فعلي من $F(x_1,\ldots,x_m)$ يحوي $F(a_1,\ldots a_n)$ ، ذلك لأن مثل هذا الحقل يجب أن يحوي F وجميع جذور $p(t)$ وهي $x_1, x_2, \ldots, x_n$. مما يجعله يساوي $F(x_1,\ldots,x_n)$. لذا نرى أن $F(x_1,\ldots x_n)$ هو حقل الانشطار لكثيرة الحدود $p(t)=t^n-a_1t^{n-1}+\ldots+(-1)^na_n$ على الحقل $F(a_1,\ldots,a_n)$. لما كانت درجة $p(t)$ تساوي n فوفقا لمبرهنة (٥-٣-٢) نحصل على $[F(x_1,\ldots,x_n):F(a_1,\ldots a_n)]\leqslant n!$ لذا نكون قد برهنا على ما نريده. نوجز ما شرحناه أعلاه بالنتيجة الأساسية المهمة التالية.

مبرهنة (٥-٦-٣)

ليكن F حقلا و $F(x_1,\ldots,x_n)$ حقل الدوال النسبية في $x_1,\ldots,x_n$ على F. ليكن S حقل الدوال النسبية المتناظرة عندئذ

١ - $[F(x_1,\ldots x_n):S]=n!$

٢ - $G(F(x_1,\ldots,x_n),S)=S_n$ *حيث S_n هي زمرة التناظر من الدرجة n.*

٣ - *إذا كانت $a_1,\ldots,a_n$ هي الدوال المتناظرة الابتدائية في $x_1,\ldots,x_n$ فإن* $S=F(a_1,a_2,\ldots,a_n)$

٤ - *الحقل $F(x_1,\ldots,x_n)$ هو حقل انشطار كثيرة الحدود* $t^n-a_1t^{n-1}+a_2t^{n-2}+\ldots+(-1)^na_n$ *على الحقل* $F(a_1,\ldots,a_n)=S$.

لقد ذكرنا سابقا أنه لأي عدد صحيح n يمكن إنشاء حقل وكثيرة حدود درجتها تساوي n على ذلك الحقل بحيث إن درجة حقل انشطار كثيرة الحدود هي أكبر ما يمكن، أي !n على الحقل المنشأ. إن مبرهنة (٥-٦-٣) تعطينا مثالا واضحا على ذلك، فإذا جعلنا $S=F(a_1,\ldots,a_n)$ واعتبرنا حقل انشطار كثيرة الحدود $t^n-a_1t^{n-1}+a_2t^{n-2}+\ldots+(-1)^na_n$ على S ، فإن درجة هذا الحقل على S تساوي !n.

إن الجزء الثالث من مبرهنة (٥-٦-٣) هو مبرهنة تقليدية. *إنها تؤكد أن أية دالة نسبية متناظرة في n من المتغيرات هي دالة نسبية في الدوال المتناظرة الابتدائية من هذه المتغيرات*. من الممكن برهان نتيجة أدق من ذلك وهي: أن أي كثيرة حدود متناظرة في n من المتغيرات هي كثيرة حدود في الدوال المتناظرة الابتدائية لهذه المتغيرات (انظر مسألة ٧). تُعرف هذه النتيجة *بمبرهنة كثيرات الحدود المتناظرة*.

في الأمثلة التي ناقشناها حول زمر التماثلات الذاتية للحقول والحقول المثبتة من قِبل هذه الزمر، وجدنا أنه من الممكن أن يكون الحقل F أصغر من الحقل المثبت من قِبل الزمرة F(K,F). من المؤكد أن F دائمًا محتوى في الحقل المثبّت، ولكن لا يُشْترط أن يساويه. لذا فإن اشتراطنا أن يكون F الحقل المثبت من قِبل الزمرة G(K,F)

لامتداد K من F يمثل تقييدًا حقيقيًا لطبيعة الامتداد K. إن اهتمامنا سينصب على مثل هذه الامتدادات.

تعريف:

يسمى K امتدادًا ناظميًا (normal extension) لـ F ، إذا كان K امتدادًا منتهيًا لـ F بحيث أن F هو الحقل المثّبت من قِبل الزمرة $G(K,F)$.

وبعبارة أخرى، إذا كان K امتدادًا ناظميًا لـ F فإن كل عنصر في K وليس في F يجب أن يكـون له صورة تختلف عنه تحت تأثير عنصر من $G(K,F)$. في الأمثلة التي ناقشنـاها كان المثالان (٥-٦-١) و(٥-٦-٣) لامتدادين ناظميين بينما المثال (٥-٦-٢) ليس كذلك.

إن فرضية كون الامتداد ناظميًا تمكننا من حساب الحقل المثّبت من قِبل أي زمرة جزئية من $G(K,F)$ بدقة كبيرة، وعلى وجه الخصوص، يمكننا تقوية مبرهنة (٥-٦-٢) لتصبح المتباينة الواردة فيها مساواة.

مبرهنة (٥-٦-٤)

ليكن K امتدادًا ناظميًا لـ F و H زمرة جزئية من $G(K,F)$ ، ليكن

$$K_H=\{x\in K/\sigma(x)=x \text{ لجميع } \sigma\in H\}$$

الحقل المثبت من قِبل H. عندئذ

١ - $[K:K_H]=0(H)$

٢ - $H=G(K,K_H)$

على وجه الخصوص، عندما $H=G(K,F)$ ، فإن $[K:F]=0(G(K,F))$

البرهان

لما كان كل عنصر في H يترك عناصر K_H ثابتة. فمن المؤكد أن $H\subset G(K,K_H)$. وفقا لمبرهنة (٥-٦-٢) نعلم أن $[K:K_H]\geqslant 0(G(K,K_H))$. وحيث إن

$$0(G(K,K_H))\geqslant 0(H)$$

نحصل على المتباينة

$$[K:K_H]\geqslant 0(G(K,K_H))\geqslant 0(H)$$

لو أمكننا بيان أن $[K:K_H]=0(H)$ ، ويتبع ذلك أن $0(H)=0(G(K,K_H))$ لاستنتجنا أن $H=G(K,K_H)$ ، لأن H زمرة جزئية من $G(K,K_H)$. لذا كي نثبت هذه المبرهنة يجب فقط أن نبرهن على أن $[K:K_H]=0(H)$.

وفقا لمبرهنة (٥ـ٥ـ١) يوجد عنصر a في K بحيث $K=K_H(a)$. هذا العنصر a يجب أن يحقق كثيرة حدود غير مختزلة على K_H درجتها تساوي m. حيث $m=[K:K_H]$ ، ولا يحقق كثيرة حدود ذات درجة أقل من ذلك (مبرهنة ٥ـ١ـ٣). دع عناصر H تكون $\sigma_1,\sigma_2,\ldots,\sigma_h$ حيث σ_1 هو العنصر المحـايد لـ $G(K,F)$ وحيث $h=0(H)$. لنعتبر الدوال المتناظرة الابتدائية للعناصر $a=\sigma_1(a),\sigma_2(a),\ldots,\sigma_n(a)$ ، أي

$$\alpha_1=\sigma_1(a)+\sigma_2(a)+\ldots+\sigma_n(a)=\sum_{i=1}^{n}\sigma_i(a)$$

$$\alpha_2=\sum_{i<j}\sigma_i(a)\sigma_j(a)$$

$$\vdots$$

$$\alpha_h=\sigma_1(a)\sigma_2(a)\ldots\sigma_h(a)$$

إن كـل α_i تبقى دون تغيـير تحت تأثـير أي عنصر σ في H (برهـن ذلك). لذا فإن $\alpha_1,\alpha_2,\ldots,\alpha_n$ عناصر في K_H حسب تعريف K_H. ولكن a (وكذلك $\sigma_2(a),\ldots\sigma_n(a)$) جذر لكثيرة الحدود

$$p(x)=(x-\sigma_1(a))(x-\sigma_2(a))\ldots(x-\sigma_h(a))$$
$$=x^h-\alpha_1x^{h-1}+\alpha_2x^{h-2}+\ldots+(-1)^h\alpha_h$$

التي معـاملاتـها تقـع في K_H. وفـقا لطبيعـة a فإن هذا يجعـل $h\geqslant m=[K:K_H]$ وعليه يكون $0(H)\geqslant[K:K_H]$. وحيث إننا نعلم أن $0(H)\leqslant[K:K_H]$ لذا نحصل على أن $0(H)=[K:K_H]$ وهذا ما نريد استنتاجه.

عندما تكون $H=G(K,F)$ فإننا نحصل على $[K:F]=0((G,F))$ لأنه في هذه الحالة $K_H=F$ بسبب *كون K امتدادًا ناظميًا من F*. إننا نقترب بسرعة من المبرهنة الأساسية في نظرية جالوا. إن ما ينقصنا هو العلاقة بين حقل الانشطار والامتداد الناظمي وهذا هو فحوى المبرهنة التالية.

مبرهنة (٥-٦-٥)

يكون K امتدادًا ناظميًا لـ F إذا وفقط إذا كان K حقل انشطار لكثيرة حدود على F.

البرهان

إن أحد اتجاهي البرهان يذكّرنا ببرهان مبرهنة (٥-٦-٤) لنفرض أن K امتداد ناظمي لـ F وفقًا لمبرهنة (٥-٥-١) فإن $K=F(a)$. لنعتبر كثيرة الحدود $p(x)=(x-\sigma_1(a))(x-\sigma_2(a))\ldots(x-\sigma_n(a))$ على K ، حيث $\sigma_1,\sigma_2,\ldots\sigma_n$ هي كل عناصر $G(K,F)$. بفك $p(x)$ نرى أنها تساوي $x^n-\alpha_1x^{n-1}+\alpha_2x^{n-2}+\ldots+(-1)^n\alpha_n$ حيث $\alpha_1,\ldots,\alpha_n$ هي الدوال المتناظرة الابتدائية للعناصر $a=\sigma_1(a),\sigma_2(a),\ldots,\sigma_n(a)$. ولكن حينئذ تصبح العناصر $\alpha_1,\ldots,\alpha_n$ غير متغيرة تحت تأثير كل σ في $G(K,F)$ وبناءً عليه فإنها تقع في F لأن K امتداد ناظمي لـ F. إذن K يشطر كثيرة الحدود $p(x)$ في $F[x]$ إلى حاصل ضرب عوامل خطية. لما كان a جذرًا لـ $p(x)$ وكان a يولد K على F فلا يمكن لـ a أن يكون في أي حقل جزئي فعلي من K يحوي F. لذا فإن K هو حقل انشطار $p(x)$ على F.

الآن نبرهن الاتجاه الآخر والذي يبدو معقدًا بعض الشيء. إننا نفضل أن نفرد جزءا من البرهان في التمهيدية التالية.

تمهيدية (٥-٦-٣)

ليكن K حقل انشطار $f(x)$ في $F[x]$ وليكن $p(x)$ عاملا غير مختزل لـ $f(x)$ في $F[x]$. إذا كانت جذور $p(x)$ هي $\alpha_1,\ldots,\alpha_r$ فإنه لكل i يوجد تماثل ذاتي σ_i في $G(K,F)$ بحيث $\sigma_i(\alpha_1)=\alpha_i$.

البرهان

لما كان كل جذر لـ $p(x)$ هو جذر لـ $f(x)$ فيجب أن يقع في K. ليكن α_i ، α_1 جذرين اختياريين لـ $p(x)$ ووفقا بمرهنة (٥-٣-٣) يوجد تماثل τ من $F_1=F(\alpha_1)$ على $F'_1=F(\alpha_i)$ ، يأخذ α_1 إلى α_i ويترك جميع عناصر F دون تغيير. الآن يمكننا اعتبار K حقل انشطار $f(x)$ ككثيرة حدود على F_1. كذلك يمكننا اعتبار K حقل انشطار $f(x)$ ككثيرة حدود على F'_1. باستخـدام المـبرهنة (٥-٣-٤) يوجـد تماثـل σ_i من K على نفسـه (أي تـماثل ذاتي لـ K) يتفق مع τ في تأثيره على F_1. ولكن عندئـذ يكون $\sigma_i(\alpha_1)=\tau(\alpha_1)=\alpha_i$ ، أي أن σ_i تترك جميع عناصر F دون تغيير. هذا ما أردنا برهانه في هذه التمهيدية.

الآن نعود لنكمل برهان مبرهنة (٥-٦-٥). لنفرض أن K هو حقل انشطار $f(x)$ في $F[x]$. نريد أن نبين أن K امتداد ناظمي لـ F. إن طريقة البرهان ستكون بالاستقراء الرياضي على $[K:F]$ والفرض أنه لكل حقلين F_1 و K_1 بحيث $[K_1:F_1]<[K:F]$ وإذا كان K_1 حقل انشطار على F_1 لكثيرة حدود في $F_1[x]$ فإن K_1 امتداد ناظمي لـ F_1.

إذا انشطرت $f(x)$ في $F[x]$ إلى عوامل خطية فإن $K=F$ وهو بالطبع امتداد ناظمي لـ F. لذا نفـرض أن لـ $f(x)$ عامـلاً غير مختزل $p(x)$ في $F[x]$ درجته $r>1$. إن الجذور *المختلفة* $\alpha_1,\alpha_2,\ldots,\alpha_r$ لـ $p(x)$ والتي عددها r كلها تقع في K و K هو حقل انشطار $f(x)$ باعتبارها كثيرة حدود على $F(\alpha_1)$. ولما كان

$$[K:F(\alpha_1)]=\frac{[K:F]}{[F(\alpha_1):F]}=\frac{n}{r}<n$$

فباستعمال فرضية الاستقراء يكون K امتدادا ناظميا لـ $F(\alpha_1)$.

ليكن العنصر θ في K مثبَّتا من قبل كل تماثل ذاتي σ في $G(K,F)$. إننا نريد أن نثبت أن θ تقع في F. لاحظ أن كل تماثل ذاتي في $G(K,F(\alpha_1))$ يترك جميع عناصر F دون تغيير، وعليه فإنه يثبِّت θ. لما كان K ناظميا على $F(\alpha_1)$ فهذا يقتضي أن تكون θ في $F(\alpha_1)$. لذا

$$\theta=\lambda_0+\lambda_1\alpha_1+\lambda_2\alpha_1^2+\ldots+\lambda_{r-1}\alpha_1^{r-1} \qquad (1)$$

حيث $\lambda_0,\ldots,\lambda_{r-1}$ في F.

وفقـا لتمهيدية (٥-٦-٣) يوجـد تماثـل ذاتي σ_i للحقـل K أي $\sigma_i \in G(K,F)$ بحيث $\sigma_i(\alpha_1)=\alpha_i$. لما كان σ_i يترك θ وكل λ_j دون تغيير فبتطبيقه على (١) نحصل على

$$\theta=\lambda_0+\lambda_1\alpha_i+\lambda_2\alpha_i^2+\ldots+\lambda_{r-1}\alpha_i^{r-1} \quad (٢)$$

لكل $i=1,2,..,r$. لذا فإن كثيرة الحدود

$$q(x)=\lambda_{r-1}x^{r-1}+\lambda_{r-2}+x^{r-2}\ldots+\lambda_1x+(\lambda_0-\theta)$$

في $K[x]$ والتي درجتها لا تزيد عن r-1 لها من الجذور المختلفـة، وهي $\alpha_1, \alpha_2,\ldots,\alpha_r$. إن هذا غير ممكن إلا إذا كانت جميع معاملات $q(x)$ تساوي صفرا. وعلى الخصوص $\lambda_0-\theta=0$ أي $\theta=\lambda_0$ مما يجعـل θ في F. هذا يكمل الاستقراء ويبرهن على أن K امتداد ناظمي لـ F. وبذا نكون قد برهنا مبرهنة (٥-٦-٥) كاملة.

تعريف

*لتكن $f(x)$ كثيرة حدود في $F[x]$ و K حقل انشطار $f(x)$ على F. نُعَرِّف **زمرة جالوا** (Galois group) لـ $f(x)$ على أنها الزمرة $G(K,F)$ المكونة من جميع التماثلات الذاتية لـ K التي تترك جميع عناصر F دون تغيير.*

لاحظ أنه يمكن اعتبار زمرة جالوا لـ $f(x)$ بأنها زمرة تبديلات لجذوره، ذلك لأنه إذا كان α جذرًا لـ $f(x)$ و σ في $G(K,F)$ فإن $\sigma(\alpha)$ جذرًا لـ $f(x)$ أيضا.

الآن نـأتي إلى النتيجـة المعـروفـة **بالمبرهنـة الأسـاسيـة لنظـريـة جالـوا** (fundamental theorem of Galois theory) إنها تنشيء تقابلاً بين الحقول الجزئية من حقل انشطار $f(x)$ والزمر الجزئية من زمرة جالوا له. بالاضافة إلى ذلك، إنها تعطينا معيارا لمعرفة كون حقل جزئي من امتداد ناظمي امتدادًا ناظميًا لـ F. سنستخدم هذه المبرهنة الأساسية في البند القادم للحصول على شروط *قابلية الحل باستخلاص الجذور* لكثيرة حدود ما.

مبرهنة (٥-٦-٦)

لتكن $f(x)$ كثير حدود في $F[x]$ و K حقل انشطار $f(x)$ على F و $G(K,F)$ زمرة جالوا له . لكل حقل جزئي T من K حاوي لـ F دع

$.G(K,T)=\{\sigma\in G(K,F)|\sigma(t)=t$ لجميع $t\in T\}$

ولكل زمرة جزئية H من $G(K,F)$ دع

$.K_H=\{x\in K|\sigma(x)=x$ لكل $\sigma\in H\}$

عندئذ فإن اقتران T بـ $G(K,T)$ يكون تقابلا بين مجموعة الحقول الجزئية من K الحاوية لـ F وبين مجموعة الزمر الجزئية من $G(K,F)$ بحيث

١ - $.T=K_{G(K,T)}$

٢ - $.H=G(K,K_H)$

٣ - $[K:T]=0(G(K,T))$ ، $[T:F]$ يساوي دليل $G(K,T)$ في $G(K,F)$.

٤ - يكون T امتدادًا ناظميًا لـ F إذا وفقط إذا كانت $G(K,T)$ زمرة جزئية ناظمية من $.G(K,F)$

٥ - عندما يكون T امتدادًا ناظميًا لـ F فإن $G(T,F)$ تماثل $G(K,F)/G(K,T)$.

البرهان

لما كان K حقل انشطار لـ f(x) على F فهو حقل انشطار لـ f(x) على أي حقل جزئي T يحوي F. إذن باستعمال مبرهنة (٥-٦-٥) يكون K امتدادًا ناظميًا لـ T. ولكن من تعريف الناظمية يكون T الحقل المثبت من قِبل G(K,T) أي $T=K_G(K,T)$ مما يبرهن الجزء ١ .

لما كان K امتدادًا ناظميًا لـ F فوفقًا لمبرهنة (٥-٦-٤) إذا أُعْطينا زمرة جزئية H من G(K,F) فإن $H=G(K,K_H)$ وهذا هو فحوى الجزء ٢ . بالإضافة إلى ذلك فإن هذا يبيّن أن أية زمرة جزئية من G(K,F) تظهر على الشكل G(K,T). لذا فإن اقتران T بـ G(K,T) يطبق مجموعة جميع الحقول الجزئية من K الحاوية على F على مجموعة جميع الزمر الجزئية من G(K,F). من الواضح أن هذا التطبيق أحادي ، لأنه إذا كانت $G(K,T_1)=G(K,T_2)$ فإنه وفقا للجزء ١ يكون

$$T_1=K_{G(K,T_1)}=K_{G(K,T_2)}=T_2$$

لما كان K امتداداً ناظمياً لـ T. فمرة أخرى، باستعمال مبرهنة (٥-٦-٤) يكون

$$[K:T]=0(G(K,T))$$

ولكن حينئذ يكون لدينا

$$0(G(K,F))=[K:F]=[K:T][T:F]=0(G(K,T))[T:F]$$

وعليه يكون

$$[T:F]=\frac{0(G(K,F))}{0(G(K,T))}$$

حيث إن الطرف الأيسر يساوي دليل $G(K,T)$ في $G(K,F)$. وهذا يثبت الجزء ٣ من المبرهنة.

إن الأجزاء التي بقي علينا برهانها هي تلك المتعلقة بخاصية الناظمية. **أولاً**: نود ملاحظة ما يلي، يكون T امتداداً ناظمياً لـ F إذا وفقط إذا كان $\sigma(T)\subset T$ لكل σ في $G(K,F)$. لغرض إثبات ذلك لاحظ أنه وفقا لمبرهنة (٥-٥-١) يكون $T=F(a)$ وعليه إذا كان $\sigma(T)\subset T$ ، فإن $\sigma(a)\in T$ لكـل σ في $G(K,F)$. ولكننـا كما رأينـا في برهان مبرهنة (٥-٦-٥) أن هذا يقتضي أن يكون T حقل انشطار لكثيرة الحدود

$$p(x)=\prod_{\sigma\in G(K,F)}(x-\sigma(a))$$

التي معـاملاتها في الحقل F. لما كان T حقل انشطار لكثيرة حدود على F فوفقاً لمبرهنة (٥-٦-٥) يكون امتداداً ناظمياً لـ F. ومن جهة أخرى إذا كان T امتداداً ناظمياً لـ F ، فإن $T=F(a)$ حيث إن جذور $p(x)$ كثيرة الحدود الدنيا لـ a على F كلها تقع في T (مبرهنة (٥-٦-٥). ولكن لكل σ في $G(K,F)$ يكون $\sigma(a)$ جذراً لـ $p(x)$ وعليه يقع $\sigma(a)$ في T. لما كان T مولَّدا من قبل a على F فإننا نحصل على $\sigma(T)\subset T$ لكل σ في $G(K,F)$.

لذا فإن T امتداد ناظمي لـ F إذا وفقط إذا كان لأي σ في $G(K,F)$ و τ في $G(K,T)$ و t في T ، $\sigma(t)$ في T وعليه $\tau(\sigma(t))=\sigma(t)$. أي إذا وفقط إذا كان $\sigma^{-1}\tau\sigma(t)=t$. وهذا يعني أن T ناظمي على F إذا وفقط إذا $\sigma^{-1}G(K,T)\sigma\subset G(K,T)$ لكل σ في $G(K,F)$ إن هذا الشرط الأخير هو بالضبط ما يجعل $G(K,T)$ زمرة جزئية ناظمية من $G(K,F)$ مما يثبت الجزء ٤ من المبرهنة.

وأخيراً إذا كان T ناظميًّا على F فإنه لأي σ في $G(K,F)$ نعلم أن $\sigma(T)\subset T$ مما يجعل σ تعـرف تماثـلاً ذاتـيًّا $\sigma.$ لـ T على الـنـحـو $\sigma.(t)=\sigma(t)$ لكـل t في T. كما أن $\sigma.$ يترك عناصر F دون تغيير فيجب أن يكون $\sigma.$ في $G(T,F)$. كذلك من الواضح أنه لكل σ و Ψ في $G(K,F)$ يكـون $(\sigma\Psi).=\sigma.\Psi.$ وعـليه فإن الـتـطبيق $\sigma\rightarrow\sigma.$ من $G(K,F)$ إلى $G(T,F)$ هو تشاكل من $G(K,F)$ إلى $G(T,F)$. ما هي نواة هذا التشاكل؟ إنها تحوي جميع العنـاصر σ في $G(K,F)$ بحيث $\sigma.$ هو التطبيق المحايد على T. أي أن النواة هي مجموعة العناصر σ في $G(K,F)$ بحيث $t=\sigma.(t)=\sigma(t)$. من تعريف هذه المجموعة نستنتج أن النواة هي بالضبط $G(K,T)$. إن صورة $G(K,F)$ في $G(T,F)$ تماثل $G(K,F)/G(K,T)$ (حسب مبرهنة (٢-٧-١)) والذي رتبته $0(G(K,F))/0(G(K,T))$ تساوي $[T:F]$ (وفقًا للجزء ٣) وهذا يساوي $0(G(T,F))$ (وفقًا لمبرهنة (٥-٦-٤)). لذا فإن صورة $G(K,F)$ في $G(T,F)$ هي جميع $G(T,F)$ وعليه نستنتج أن $G(T,F)$ يماثل $G(K,F)/G(K,T)$. هذا ينهي برهان الجزء الخامس مما يكمّل برهان مبرهنة (٥-٦-٦).

مسـائـل

١ - إذا كان K حقلاً و S مجموعة من التماثلات الذاتية لـ K. فبرهن على أن الحقل المثبَّت من قِبل S يساوي الحقل المثبَّت من قبل $\bar{S}$. (الزمرة الجزئية من زمرة جميع التماثلات الذاتية لـ K والمولَّدة بواسطة S).

٢ - برهن تمهيدية (٥-٦-٢).

٣ - باستخدام معيار ايزنشتاين. أثبت أن كثيرة الحدود $x^4+x^3+x^2+x+1$ غير مختزلة على حقل الأعداد النسبية.

٤ - في مثال (٥-٦-٣). برهن على أن كل تطبيق σ_i يُعرِّف تماثلاً ذاتيًا لـ $F_0(\omega)$.

٥ - في مثال (٥-٦-٣). برهن على أن الحقل المثبَّت في $F_0(\omega)$ تحت تأثير $\sigma_1,\sigma_2,\sigma_3,\sigma_4$ هو بالضبط F_0.

٦ - برهن بصورة مباشرة على أن أي تماثل ذاتي لـ K يجب أن يترك أي عدد نسبي دون تغيير.

*٧ - برهن على أن كثـيرة الحـدود المتنـاظرة في $x_1,\ldots,x_n$ هي كثيرة حدود في الدوال الابتدائية المتناظرة في $x_1,\ldots,x_n$.

٨ - عبِّر عمّا يلي بكثيرات حدود في الدوال المتناظرة الابتدائية في x_1,x_2,x_3

(ا) $x_1^2+x_2^2+x_3^2$.

(ب) $x_1^3+x_2^3+x_3^3$.

(جـ) $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$

٩ - إذا كانت $\alpha_1,\alpha_2,\alpha_3$ جذورا لكثيرة الحدود التكعيبية x^3+7x^2-8x+3 فأوجد كثيرة الحدود التكعيبية التي جذورها

(ا) $\alpha_1^2,\alpha_2^2,\alpha_3^2$. (ب) $\frac{1}{\alpha_1},\frac{1}{\alpha_2},\frac{1}{\alpha_3}$ (جـ) $\alpha_1^3,\alpha_2^3,\alpha_3^3$.

١٠* - برهن **متطابقات نيوتن** (Newton's identities) أي إذا كانت $\alpha_1,\alpha_2,\ldots,\alpha_n$ جذور كثيرة الحدود $f(x)=x^n+a_1x^{n-1}+a_2x^{n-1}+\ldots+a_n$ وكان $s_k=\alpha_1{}^k+\alpha_2{}^k+\ldots+\alpha_n{}^k$ فإن

(ا) $s_k+a_1\ s_{k-1}+a_2s_{k-2}+\ldots+a_{k-1}s_1+ka_k=0$ عندما $k=1,2,\ldots,n$

(ب) $s_k+a_1s_{k-1}+\ldots+a_ns_{k-n}=0$ لكل $k>n$

(جـ) عندما $n=5$ استعن بجزء (ا) لتعيين s_2,s_3,s_4,s_5

١١ - أثبت أن الدوال المتناظرة الابتدائية في $x_1,\ldots,x_n$ هي حقا دوال متناظرة في $x_1,\ldots,x_n$.

١٢ - إذا كان $p(x)=x^n-1$. فبرهن على أن زمرة جالوا لـ $p(x)$ على حقل الأعداد النسبية هي زمرة إبدالية.

يطلق على العدد المركب ω اسم **جذر بدائي للواحد من رتبة n** (Primitive n*th* root of unity) إذا كان $\omega^n=1$ و $\omega^m\neq1$ حيث $0<m<n$.

فيما سيأتي سيعني F_0 حقل الأعداد النسبية.

١٣ - (ا) برهن على أنه يوجد $\phi(n)$ من الجذور البدائية للواحد من رتبة n ، حيث $\phi(n)$ هي دالة ايلر (Euler function).

(ب) إذا كان ω جذرًا بدائيًا للواحد من رتبة n فبرهن على أن $F_0(\omega)$ هو حقل انشطار x^n-1 على F_0 (وبذا يكون امتدادًا ناظميًا لـ F_0).

(جـ) إذا كانت $\omega_1,\dots,\omega_{\phi(n)}$ هي الجذور البدائية للواحد من رتبة n. فبرهن على أن أي تماثل ذاتي لـ $F_0(\omega_1)$ يأخذ ω_1 إلى w_i حيث $1\leqslant i\leqslant \phi(n)$.

(د) برهن على أن $[F_0(\omega_1):F_0]\leqslant \phi(n)$.

١٤ ـ الرموز هنا كما هي في مسألة (١٣).

(أ*) برهن على أنه يوجد تماثل ذاتي σ_i للحقل $F_0(\omega_1)$ بأخذ ω_1 إلى ω_i.

(ب) برهن على أن معاملات كثيرة الحدود $p_n(x)=(x-\omega_1)(x-\omega_2)\dots(x-\omega_{\phi(n)})$ أعـداد نسبيـة (يُطلق على كثيرة الحدود $p_n(x)$ اسـم *كثيرة الحـدود الـدورية* cyclotomic polynomial من رتبة n).

(جـ*) أثبت أن معاملات $p_n(x)$ هي في الحقيقة أعداد صحيحة.

١٥** ـ استعمل نتائج المسألتين (١٣) و (١٤) لكي تبرهن على أن $p_n(x)$ غير مختزلة على F_0 لكل $n\geqq 1$ (انظر مسألة ٨ في بند ٣).

١٦ ـ احسب $p_n(x)$ لقيم $n=3,4,6,8$. برهن على أن معاملات كل منها أعداد صحيحة وأثبت مباشرة أنها غير مختزلة على F_0.

١٧ ـ (ا) برهن على أن زمرة جالوا لـ x^3-2 على F_0 تماثل S_3 زمرة التناظر من الدرجة 3.

(ب) أوجد حقل انشطار x^3-2 على F_0.

(جـ) لكل زمرة جزئية H من S_3 أوجد K_H وتأكد من التقابل المذكور في مبرهنة (٥-٦-٦).

(د) أوجد امتدادًا ناظميًا في K من الدرجة 2 على F_0.

١٨ ـ إذا احتوى الحقل F على جذر بدائي للواحد من رتبة n. فبرهن على أن زمرة جالوا لـ x^n-a إبدالية، حيث a في F.

(٥ ـ ٧) قابلية الحل باستخلاص الجذور

إذا كان لدينـا كثـيرة الحـدود x^2+3x+4 على حقل الأعداد النسبية F_0 ، فمن الصيغة التربيعية نعلم أن جذريها هما $(-3\pm\sqrt{-7})/2$. لذا فإن الحقل $F_0(\sqrt{7}i)$ هو حقل انشطار x^2+3x+4 على F_0. نستنتج من ذلك أنه يوجد عنصر $\gamma=-7$ في F_0. بحيث إن الامتداد $F_0(\omega)$ حيث $\omega^2=\gamma$ يحوي جذري كثيرة الحدود x^2+3x+4.

ومن وجهة نظر أخرى إذا كان لدينا كثيرة الحدود التربيعية *العامة* $p(x)=x^2+a_1x+a_2$ فيمكننا اعتبارها كثيرة حدود *خاصة* على $F(a_1,a_2)$ حقل الدوال النسبية في المتغيرين a_1 و a_2 على F. إن جذري كثيرة الحدود p(x) موجودان في الحقل الذي نحصل عليه بضم العنصر ω إلى $F(a_1,a_2)$ حيث $\omega^2=a_1^2-4a_2$ في $F(a_1,a_2)$. إن هناك صيغة لإيجاد جذري p(x) بدلالة a_1,a_2 والجذرين التربيعيين لدوال نسبية في a_1 و a_2.

إن الوضع بالنسبة للمعادلة التكعيبية مشابهة لما ذكر أعلاه. فإذا كان لدينا المعادلة التكعيبية العامة

$$p(x)=x^3+a_1x^2+a_2x+a_3$$

يمكننا إيجاد صيغة معيّنة لجذورها تحوي تركيبات من جذور تربيعية وتكعيبية لدوال نسبية في a_1,a_2,a_3. إن هذه الصيغة قد تكون معقدة بعض الشيء وهي معروفة باسم **صيغة كاردان** (Cardan's formula).

الآن ليكن

$$p=a_2-\frac{a_1^2}{3}$$

و

$$q=\frac{2a_1^3}{27}-\frac{a_1a_2}{3}+a_3$$

ودع

$$P=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}$$

و

$$Q=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}$$

(حيث إن الجذور التكعيبية مختارة بصورة مناسبة). إن جذور المعادلة التكعيبية هي $P+Q-(a_1/3)$ ، $\omega P+\omega^2Q-(a_1/3)$ و $w^2P+\omega Q-(a_1/3)$ حيث $\omega\neq 1$ هو جذر تكعيبي للواحد. إن الغرض من الصيغ أعلاه هو بيان أنه بضم جذر تربيعي معيّن ومن ثم جذر تكعيبي للحقل $F(a_1,a_2,a_3)$ نحصل على حقل توجد فيه جميع جذور p(x).

في حالة كثيرة الحدود من الدرجة الرابعة والتي سوف لا نقدم لجذورها صيغة صريحة فإنه يمكن اختزال المسألة إلى حل معادلة تكعيبية معيّنة وذلك باستخدام بعض

العمليات النسبية والجذور التربيعية. لذا فمن الممكن في هذه الحالة أيضا إيجاد صيغة للجذور بدلالة تركيبات من جذور تربيعية وتكعيبية لدوال نسبية من المعادلات.

أما بالنسبة لكثيرات الحدود من الدرجة الخامسة فما فوق فلا يمكن إيجاد صيغة عامة لجذورها كما في الحالات أعلاه ذلك لأننا سنبرهن فيما سيأتي استحالة ذلك.

إذا كان لدينا حقل F وكثيرة حدود $p(x)$ في $F[x]$ فنقول إن $p(x)$ قابلة للحل *باستخلاص الجذور* (solvable by radicals) على F إذا أمكننا إيجاد متتالية منتهية من الحقول $F_1=F(\omega_1)$ ، $F_2=F_1(\omega_2)$ ، $F_k=F_{k-1}(\omega_k)$ بحيث $\omega_1^{r_1}\in F$ ، $\omega_2^{r_2}\in F_1$ ، . . . ، $\omega_k^{r_k}\in F_{k-1}$ على أن تكون جميع جذور $p(x)$ واقعة في F_k.

إذا كان K حقل انشطار $p(x)$ على F فتكون $p(x)$ قابلة للحل باستخلاص الجذور إذا أمكننا إيجاد متتالية من الحقول كما في أعلاه بحيث $K\subset F_k$. هناك ملاحظة مهمة سوف نستعملها في برهان مبرهنة (٥ـ٧ـ٢) وهي أنه إذا أمكننا إيجاد F_k فيمكننا الفرض أنه امتداد *ناظمي* لـ F دون المساس بعمومية دراستنا. نترك برهان ذلك للقارىء (مسألة ١).

نعني بكثيرة الحدود العامة $p(x)=x^n+a_1x^{n-1}+\dots+a_n$ من الدرجة n على F ما يلي: ليكن $F(a_1,\dots,a_n)$ حقل الدوال النسبية في المتغيرات $a_1,\dots,a_n$ على F ولنعتبر كثيرة الحدود الخاصة $p(x)=x^n+a_1x^{n-1}+\dots+a_n$ على الحقل $F(a_1,\dots,a_n)$. نقول إن $p(x)$ قابلة للحل باستخلاص الجذور إذا كانت كذلك على $F(a_1,\dots,a_n)$. إن هذا ليعبّر حقيقة عن مفهوم «إيجاد صيغة» لجذور $p(x)$ تحوي تركيبات من مقادير على الصيغة $\sqrt[m]{g(a_1,\dots,a_n)}$.. حيث m عدد صحيح موجب و $g(a_1,\dots,a_n)$ دالة نسبية في $F(a_1,\dots,a_n)$. عندما $n=2,3,4$ أشرنا إلى إمكانية وجود مثل هذه الصيغة. في حالة $n\geq 5$ استطاع الرياضي ابيل (Abel) برهان عدم إمكانية ذلك. بيد أن هذا لا ينفي إمكانية كون كثيرة حدود ما قابلة للحل باستخلاص الجذور على F. وفي الحقيقة إننا سنقدم معيارًا لذلك

بدلالـة زمرة جالوا لكثيرة الحدود. ولكن أولا يجب علينا أن نطوّر بعض النتائج من نظرية الزمر. إن بعضا منها قُدِّم كمسائل في نهاية الفصل الثاني ولكن مع ذلك نعرضها هنا.

تعريف

*يقال عن زمرة G إنها **قابلة للحل** (solvable) إذا أمكننا إيجاد سلسلة منتهية من الزمر الجزئية $G=N_0\supset N_1\supset N_2\supset\ldots\supset N_k=(e)$ بحيث إن N_i زمـرة جزئيـة ناظميـة مـن N_{i-1} والزمرة الخارجة N_{i-1}/N_i إبدالية.*

إن كل زمرة إبدالية قابلة للحل حيث نجعل $N_0=G$ و $N_1=(e)$ لتحقق التعريف أعلاه. إن زمرة التناظر S_3 من الدرجة الثالثة قابلة للحل، ذلك لأننا إذا جعلنا $N=\{e,(1,2,3),(1,3,2)\}$ فإنها زمرة جزئية ناظمية في S_3 و S_3/N_1 و $N_1/(e)$ زمرتان إبداليتان لأن رتبتهما 2 و 3 على الترتيب. يمكن إثبات أن S_4 قابلة للحل (مسألة ٣). لقيم $n\geq 5$ سوف نبرهن في مبرهنة (٥ـ٧ـ١) على أن S_n غير قابلة للحل.

الآن نبحث عن طريقـة أخـرى لوصف قابلية الحـل. إذا كان لدينا زمرة G وعنصران a و b في G فإن **مُبَدِّل** (commutator) a و b هو العنصر $a^{-1}b^{-1}ab$. إن **زمرة المبدِّلات الجزئية** (commutator subgroup) G' في G هي الزمرة الجزئية المولدة من جميع المبدِّلات في G (ليس من الصحيح دائما أن مجموعة جميع المبدلات في زمرة G تكون زمرة جزئية فيهـا). إن أحد التمارين السابقة كان برهان أن G' زمرة جزئية ناظمية في G. بالإضافة إلى ذلك فإن الزمرة G/G' إبدالية، ذلك لأنه إذا كان bG' و aG' عنصرين فيها حيث a,b في G فإن

$$(aG')(bG')=abG'=ba(a^{-1}b^{-1}ab)G'$$

$$=baG' \quad (\text{لأن } a^{-1}b^{-1}ab \text{ في } G')$$

$$=(bG')(aG')$$

ومن جهة أخرى إذا كانت M زمرة جزئية ناظمية في G بحيث G/M إبدالية، فإن $M\supset G'$ لأنه لأي عنصرين a و b في G يكون $(aM)(bM)=(bM)(aM)$ وبالتالي فإن $baM=abM$ مما يجعل $a^{-1}b^{-1}abM=M$ أي $a^{-1}b^{-1}ab$ في M. لما كانت M تحوي جميع المبدلات فإنها يجب أن تحوي الزمرة المتولدة منها، ألا وهي G'.

إن G' زمرة بحد ذاتها، لذا يمكننا التحدث عن زمرة المبدِّلات الجزئية لها $G^{(2)}=(G')'$. إنها الـزمرة الجزئية من G المولَّدة بواسطة كل العناصر $(a')^{-1}(b')^{-1}a'b'$ حيث a' و b' في G'. من السهل البرهان أن $G^{(2)}$ زمرة جزئية ناظمية في G بالإضافة إلى كونها كذلك في G' (مسألة ٤). تستمر على هذا المنوال فنعرّف **زمر المبدِّلات الجزئية العليا** (higher commutator subgroups) $G^{(m)}$ على النحو $G^{(m)}=(G^{(m-1)})'$. إن كل $G^{(m)}$ هي زمرة جزئية ناظمية في G (انظر مسألة ٤) و $G^{(m-1)}/G^{(m)}$ زمرة إبدالية.

إن زمر المبدِّلات الجزئية العليا في G تقدم لنا معيارًا مقتضيًا لقابلية الحل وهو ما يلي.

تمهيدية (٥-٧-١)

تكون الزمرة G قابلة للحل إذا وفقط إذا كانت $G^{(k)}=(e)$ لعدد صحيح k.

البرهان

إذا كانت $G^{(k)}=(e)$ فدع $N_0=G$ ، $N_1=G'$ ، $N_2=G^{(2)}$ ، . . . ، $N_k=G^{(k)}=(e)$ ، عندئذ نحصل على

$$G=N_0\supset N_1\supset N_2\supset\ldots\supset N_k=(e)$$

حيث N_i ناظمية في N_{i-1} لأنها كذلك في G. وأخيرا

$$\frac{N_{i-1}}{N_i}=\frac{G^{(i-1)}}{G^{(i)}}=\frac{G^{(i-1)}}{(G^{(i-1)})'}$$

لذا فهي إبدالية. لذا فمن تعريف قابلية الحل نستنتج أن G قابلة للحل.

وبالعكس، إذا كانت G قابلة للحل فإنه توجد سلسلة $G=N_0\supset N_1\supset N_2\supset\ldots\supset N_k=(e)$ ولكن حينئذ تقع زمرة المبدلات الجزئية N'_{i-1}. لـ N_{i-1} في الزمرة N_i لذا $N_1\supset N'_0=G'$ ، $N_2\supset N'_1\supset(G')'=G^{(2)}$ ، $N_3\supset N'_2\supset(G^{(2)})'\supset G^{(3)}$ ، . . . ، $N_i\supset G^{(i)}$ ، $(e)=N_k\supset G^{(k)}$.
إذن فإننا نحصل على $G^{(k)}=(e)$.

نتيجة

إذا كانت G قابلة للحل وكانت $\bar{G}$ صورة تشاكلية من G فإن $\bar{G}$ قابلة للحل.

البرهان

لما كانت $\bar{G}$ صورة تشاكلية من G نستنتج على الفور أن $(\bar{G})^{(k)}$ هي صورة $G^{(k)}$. لما كانت $G^{(k)}=(e)$ لعدد ما k فإن $(\bar{G})^{(k)}=(e)$ لنفس العدد k. لذا تكون $\bar{G}$ قابلة للحل وفقًا للتمهيدية أعلاه.

إن التمهيدية القادمة تعتبر الخطوة الأساسية في برهان أن العائلة غير المنتهية من الزمر S_n غير قابلة للحل في حالة $n\geqslant5$. هنا نعني بـ S_n زمرة التناظر من الدرجة n.

تمهيدية (٥-٧-٢)

لتكن $G=S_n$ حيث $n\geqslant5$ فإن $G^{(k)}$ تحوي كل دورة طولها 3 في S_n وذلك في جميع الحالات $k=1,2,\ldots$

البرهان

أولا: نشير إلى الحقيقة أنه لأية زمرة اختيارية G إذا كانت N زمرة جزئية ناظمية فيها فإن N' زمرة جزئية ناظمية في G (مسألة ٥).

إننا ندعي أنه إذا كانت N زمرة جزئية ناظمية في $G=S_n$ حيث $n\geqslant5$ وكانت N حاوية على جميع الدورات التي طولها 3 في S_n فإن N' يجب أن يحوي جميع هذه الدورات

كذلك. فلو فرضنا أن $a=(1,2,3)$ و $b=(1,4,5)$ يقعان في N (إننا نستعمل هنا حقيقة كون $n\geqslant 5$) فإن

$$a^{-1}b^{-1}ab=(3,2,1)(5,4,1)(1,2,3)(1,4,5)=(1,4,2)$$

يقع في N' باعتباره مبدلاً. لما كانت N' زمرة جزئية ناظمية في G فإنه لأي $\pi\in S_n$ يجب أن يكون $\pi^{-1}(1,4,2)\pi$ في N' أيضا. اختر π في S_n بحيث $\pi(1)=i_1$ ، $\pi(4)=i_2$ ، $\pi(2)=i_3$ ، حيث i_1 ، i_2 و i_3 أي أعداد صحيحة مختلفة في المجال من 1 إلى n. لذا $\pi^{-1}(1,4,2)\pi=(i_1,i_2,i_3)$ يقع في N'. إذن N' تحوي جميع الدورات التي طولها 3.

إذا جعلنا $N=G$ فإنها بالتأكد ناظمية في G وتحوي جميع الدورات التي طولها 3. نستنتج من ذلك أن G' تحوي جميع الدورات التي طولها 3. وحيث إن G' ناظمية في G فإن $G^{(2)}$ تحوي جميع الدورات التي طولها 3. ولما كانت $G^{(2)}$ ناظمية في G فإن $G^{(3)}$ تحوي جميع الدورات التي طولها 3. بالاستمرار على هذا النحو نستنتج أن $G^{(k)}$ يحوي جميع الدورات التي طولها 3 لأي عدد صحيح موجب k.

كنتيجة مباشرة من التمهيدية أعلاه نذكر هذه النتيجة الشيّقة من نظرية الزمر.

مبرهنة (٥-٧-١)

إن الزمرة S_n غير قابلة للحل لقيم $n\geqslant 5$.

البرهان

إذا كانت $G=S_n$ فوفقًا لتمهيدية (٥-٧-٢)، $G^{(k)}$ تحوي جميع الدورات التي طولها 3 في S_n لأي عدد صحيح موجب k. لذا فإن $G^{(k)}\neq(e)$ لأي k ونستنتج من ذلك أن G غير قابلة للحل باستعمال تمهيدية (٥-٧-١).

الآن نربط مفهوم قابلية الحل باستخلاص الجذور لكثير حدود $p(x)$ مع قابلية الحل كزمرة، لزمرة جالوا لـ $p(x)$. إن الاصطلاحين المستخدمين يقترحان وجود مثل هذا

الارتباط. ولكن أولا نحتاج إلى نتيجة تتعلق بزمرة جالوا لنوع معيّن من كثيرات الحدود.

تمهيدية (٥-٧-٣)

لنفرض أن الحقل F يحوي جميع جذور الواحد من الدرجة n (لعدد معيّن n) وأن $a\neq 0$ في F. دع x^n-a في F[x] و K حقل انشطار x^n-a على F. عندئذ

١ - $K=F(u)$ حيث u أي جذر لـ x^n-a.

٢ - زمرة جالوا لـ x^n-a على F إبدالية.

البرهان

لما كان F يحوي جميع الجذور من الدرجة n فإنه يحوي $\zeta=e^{2\pi i/n}$. لاحظ أن $\zeta^n=1$ ولكن $\zeta^m\neq 1$ لكل $0<m<n$.

إذا كان u أي جذر لـ x^n-a في K فإن $\zeta^{(n-1)}u$ ، . . . ، ζ^2u ، ζu ، u هي جميع جذور x^n-a. إن كونها جذورا أمر واضح أما عدم تساويها فإنه نتيجة لما يلي: إذا كان $\zeta^iu=\zeta^ju$ عندما $0\leqslant i<j<n$ ، حينئذ عندما $u\neq 0$ و $(\zeta^i-\zeta^j)u=0$ ، يجب أن تكون $\zeta^i=\zeta^j$ وهذا مستحيل لأنه ينتج عنه $\zeta^{j-i}=1$ مع $0<j-i<n$. لما كان ζ في F فإن جميع العناصر $\zeta^{n-1}u$ ، . . . ، ζu ، u تقع في F(u) مما يجعل F(u) يشطر x^n-a. وحيث إنه لا يوجد حقل جزئي فعلي من F(u) يحوي F و u نستنتج أنه لا يوجد حقل جزئي فعلي من F(u) يشطر x^n-a. لذا فإن F(u) هو حقل انشطار x^n-a وعليه نكون قد برهنا على أن $K=F(u)$.

إذا كان σ و τ عنصرين في زمرة جالوا لـ x^n-a ، أي، إذا كان σ و τ تماثلين ذاتيين لـ $K=F(u)$ يتركان كل عنصر في F دون تغيير، فإنه لكون σ(u) و τ(u) جذرين لـ x^n-a يكون $\sigma(u)=\zeta^iu$ و $\tau(u)=\zeta^ju$ لعددين i و j. لذا فإن

$$\sigma\tau(u)=\sigma(\zeta^ju)=\zeta^j\sigma(u) \text{ (لأن } \zeta^j \text{ في } F\text{)} =\zeta^j\zeta^iu=\zeta^{i+j}u$$

وبصورة مشابهة ترى أن $\tau\sigma(u)=\xi^{i+j}u$. إذن $\sigma\tau$ و $\tau\sigma$ يتفقان في تأثيرهما على u وكذلك على F لذا فإنهما يتفقان على $K=F(u)$.

ولكن حينئذ يكون $\tau\sigma=\sigma\tau$ مما يجعل زمرة جالوا إبدالية.

لاحظ أن التمهيدية تقول إنه عندما يحوي F جميع جذور الواحد من الدرجة n فبضم أحد جذور x^n-a إلى F حيث a في F نحصل على حقل انشطار x^n-a مما يجعل هذا الامتداد ناظميا.

فيما تبقى من هذا البند نفترض أن F حقل يحوي جميع جذور الواحد من الدرجة n ولجميع قيم n.

مبرهنة (٥-٧-٢)

إذا كانت كثيرة الحدود $p(x)$ في $F[x]$ قابلة للحل باستخلاص الجذور على F فإن زمرة جالوا على F لـ $p(x)$ قابلة للحل.

البرهان

ليكن K حقل انشطار $p(x)$ على F. إن زمرة جالوا لـ $p(x)$ على F هي $G(K,F)$.
لما كانت $p(x)$ قابلة للحل باستخلاص الجذور فإنه توجد متتالية من الحقول.

$$F\subset F_1=F(\omega_1)\subset F_2=F(\omega_2)\subset \ldots \subset F_k=F_{k-1}(\omega_k)$$

بحيث $\omega_1^{r_1}\in F$ ، $\omega_2^{r_2}\in F_1$ ، . . . ، $\omega_k^{r_k}\in F_{k-1}$ ، وحيث $K\subset F_k$. كما أشرنا سابقا فإنه دون التأثير على عمومية المناقشة يمكن الفرض أن F_k امتداد ناظمي لـ F. ويترتب على ذلك أن F_k امتداد ناظمي لأي حقل وسطي مما يجعل F_k امتدادًا ناظميًا لكل F_i.

باستخدام تمهيدية (٥-٧-٣) نجد أن كل F_i هو امتداد ناظمي لـ F_{i-1} وحيث إن F_k ناظمي على F_{i-1} نستنتج من مبرهنة (٥-٦-٦) أن $G(F_k,F_i)$ هي زمرة جزئية ناظمية في $G(F_k,F_{i-1})$. لنعتبر السلسلة

$$G(F_k,F)\supset G(F_k,F_1)\supset G(F_k,F_2)\supset\ldots G(F_k,F_{k-1})\supset(e) \quad (1)$$

كما أشرنا الآن، إن كل زمرة جزئية في هذه السلسلة هي زمرة جزئية ناظمية في الزمرة التي تسبقها. لما كان F_i امتداداً ناظمياً من F_{i-1} فبالاستعانة بمبرهنة جالوا الأساسية (مبرهنة ٥-٦-٦) الزمرة $G(F_i,F_{i-1})$ تماثل $G(F_k,F_{i-1})/G(F_k,F_i)$. ولكن وفقا لتمهيدية (٥-٧-٣) فإن الزمرة $G(F_i,F_{i-1})$ إبدالية. لذا فإن كل زمرة خارجة $G(F_k,F_{i-1})/G(F_k,F_i)$ في السلسلة (١) هي إبدالية.

نستنتج أن الزمرة $G(F_k,F)$ قابلة للحل. لما كان $K\subset F_k$ و K امتداداً ناظمياً لـ F (لأنه حقل انشطار) فباستعمال مبرهنة (٥-٦-٦) تكون $G(F_k,K)$ زمرة جزئية ناظمية في $G(F_k,F)$ و $G(K,F)$ تماثل $G(F_k,F)/G(F_k,K)$. وعليه تكون $G(K,F)$ صورة تشاكلية من $G(F_k,F)$ القابلة للحل. لذا فبالاستعانة بنتيجة تمهيدية ٥-٧-١ نستنتج أن الزمرة $G(K,F)$ قابلة للحل. وحيث إن $G(K,F)$ هي زمرة جالوا لـ $p(x)$ على F نكون بذلك قد أثبتنا المبرهنة.

الآن نقدم ملاحظتين دون برهان

(١) إن عكس مبرهنة (٥-٧-٢) صحيح أيضا، أي إذا كانت زمرة جالوا لـ $p(x)$ على F قابلة للحل فإن $p(x)$ *قابل للحل باستخلاص الجذور على F.*

(٢) إن مبرهنة (٥-٧-٢) وعكسها صحيحان حتى لو لم يحتو F على جذور الواحد.

باستعادة ما نقصده بكثيرة الحدود العامة من الدرجة n على F، $p(x)=x^n+a_1x^{n-1}+\ldots+a_n$ وما نقصده بقابلية الحل باستخلاص الجذور، نخلص إلى المبرهنة التقليدية الرائعة للرياضي ابيل (Abel).

مبرهنة (٥-٧-٣)

لا يمكن حل كثيرة الحدود العامة من الدرجة $n\geq 5$ باستخلاص الجذور.

البرهان

لقد رأينا في مبرهنة (٥-٦-٣) أنه إذا كان $F(a_1,...,a_n)$ حقل الدوال النسبية في المتغيرات $a_1,...,a_n$ ، فإن زمرة جالوا لكثيرة الحدود $p(t)=t^n+a_1t^{n-1}+...+a_n$ على $F(a_1,...,a_n)$ هي S_n زمرة التناظر من الدرجة n. باستخدام مبرهنة (٥-٧-١) نجد أن S_n زمرة غير قابلة للحل عندما $n\geq5$. لذا فوفقًا لمبرهنة (٥-٧-٢) تصبح $p(t)$ غير قابلة للحل باستخلاص الجذور على $F(a_1,...,a_n)$ عندما $n\geq5$.

مسـائـل

١ - إذا كانت $p(x)$ قابلة للحل باستخلاص الجذور على F. فبرهن على وجود متتالية من الحقول

$$F\subset F_1=F(\omega_1)\subset F_2=F_1(\omega_2)\subset...\subset F_k=F_{k-1}(\omega_k)$$

بحيث $\omega_1^{r_1}\in F$ ، $\omega_2^{r_2}\in F_1$ ، . . . ، $\omega_k^{r_k}\in F_{k-1}$ و F_k يحوي جميع جذور $p(x)$ بحيث يكون F_k امتدادًا ناظميًا لـ F.

٢ - برهن على أن أية زمرة جزئية من زمرة قابلة للحل هي زمرة قابلة للحل.

٣ - أثبت أن S_4 زمرة قابلة للحل.

٤ - إذا كانت G زمرة. فبرهن على أن جميع الزمر $G^{(k)}$ هي زمر جزئية ناظمية من G.

٥ - إذا كانت N زمرة جزئية ناظمية من G. فأثبت أن N' يجب أن تكون زمرة جزئية ناظمية من G.

٦ - برهن على أن الزمرة المتناوبة A_n (زمرة التبديلات الزوجية في S_n) لا تحوي زمرة جزئية ناظمية غير تافهة لجميع قيم $n\geq5$.

(٥ - ٨) زمر جالوا على حقل الأعداد النسبية

لقد رأينا في مبرهنة (٥-٣-٢) أنه إذا كان لدينا حقل F وكثيرة حدود $p(x)$ من الدرجة n في $F[x]$ فإن درجة حقل انشطار $p(x)$ على F لا تزيد عن $n!$. في البند السابق وجدنا أنه هناك حقل F وكثيرة حدود $p(x)$ من الدرجة n على F بحيث إن درجة حقل انشطار $p(x)$ على F تساوي $n!$. في الحقيقة إذا كان F_0 أي حقل و F حقل الدوال النسبية

في المتغيرات $a_1,\dots,a_n$ على F_0 فقد بينا أن درجة حقل الانشطار K لكثير الحدود $p(x)=x^n+a_1x^{n-1}+\dots+a_n$ على F تساوي $n!$ بالضبط. وبالإضافة إلى ذلك بيّنا أن زمرة جالوا لـ K على F هي S_n زمرة التناظر من الدرجة n. إن هذه الحقيقة هي الأساس الذي اعتمدنا عليه في أن كثيرة الحدود العامة من الدرجة $n\geqslant 5$ غير قابلة للحل باستخلاص الجذور.

ومع ذلك، يبدو من المستحسن معرفة أن الظاهرة التي وصفت أعلاه تحدث مع حقول نألفها أكثر من حقل الدوال النسبية في n من المتغيرات. إن الذي سنفعله، على الأقل، هو إثبات أنه لأي عدد أولي p يمكننا إيجاد كثيرة حدود من الدرجة p على حقل الأعداد النسبية بحيث إن درجة حقل انشطارها على الأعداد النسبية تساوي $p!$. بهذه الطريقة سنحصل على كثيرة حدود معاملاتها أعداد نسبية وزمرة جالوا لها على الأعداد النسبية هي S_p. على ضوء مبرهنة (٥-٧-٢) نستنتج من هذا أنه لا يمكن الحصول على جذور كثيرة الحدود المعنية على شكل تركيبات من جذور نونية لأعداد تشتمل على أعداد نسبية بالرغم من أننا استخدمنا حقيقة كون جذور الواحد موجودة في الحقل لغرض إثبات مبرهنة (٥-٧-٢) وأن جذور الواحد لا تقع في الأعداد النسبية فإننا نستخدم هنا الملاحظة (٢) التي تلت برهان مبرهنة (٥-٧-٢) أي أن مبرهنة (٥-٧-٢) تبقى صحيحة حتى في حالة غياب جذور الواحد.

إننا سنستخدم الحقيقة القائلة إن جميع جذور كثيرة الحدود التي معاملاتها أعداد نسبية تقع في حقل الأعداد المركبة.

والآن نبرهن على ما يلي.

مبرهنة (٥-٨-١)

لتكن $q(x)$ كثيرة حدود غير مختزلة من الدرجة p على حقل الأعداد النسبية Q، حيث p عدد أولي. ولنفرض أن لـ $q(x)$ بالضبط جذرين غير حقيقيين في حقل

الأعـداد المـركبـة، عنـدئذ تكون زمرة جالوا لـ $q(x)$ على Q هي S_p زمرة التناظر من الدرجة p. إن درجة حقل انشطار $q(x)$ على Q تساوي $p!$.

البرهان

ليكن K حقـل انشطار $q(x)$ على Q. لما كانت $q(x)$ غير مختزلة على Q فإنه إذا كان α جذرا لها تصبح $[Q(\alpha):Q]=p$ وفقا لمبرهنة (٥-١-٣). وحيث إن $K\supset Q(\alpha)\supset Q$ فباستعمال مبرهنة (٥-١-١) نحصل على $[K:Q]=[K:Q(\alpha)][Q(\alpha):Q]=[K:Q(\alpha)]p$ مما يجعل $p|[K:Q]$. إذا كانـت G زمـرة جالـوا لـ K على Q فوفـقًـا لمبرهـنـة (٥-٦-٤) يكـون $0(G)=[K:Q]$. لذا فإن $p|0(G)$ ، وبـنـاءً عليه فإن G تحوي عنصرا σ رتبته p باستخدام مبرهنة كوشي (مبرهنة ٢-١١-٣).

إلى هذا الحد لم نستعمل بعد فرضيتنا التي تنص على أن لـ $q(x)$ بالضبط جذرين غير حقيقيين. نقـوم باستخـدامهـا الآن. إذا كان α_1,α_2 هما هذان الجـذران غير الحقيقيين، فإن $\alpha_2=\bar{\alpha}_1,\alpha_1=\bar{\alpha}_2$ (مسألة ١٣ في بند ٥-٣) حيث $\bar{\alpha}_i$ يعني المرافق المركب لـ $\alpha_i(i=1,2)$. إذا كانت $\alpha_3,\ldots,\alpha_p$ هي الجـذور الأخـرى لـ $q(x)$ فلكونها أعدادًا حقيقية يكون $\bar{\alpha}_i=\alpha_i$ لكل $i\geqslant 3$. لذا فإن تطبيق الأعداد المركبة الذي يأخذ كل عدد لمرافقه هو تطبيق من K إلى نفسه وهو تماثل ذاتي τ لـ K على Q يبادل α_1 و α_2 بينما يترك جميع الجذور الأخرى لـ $q(x)$ مثبّتة.

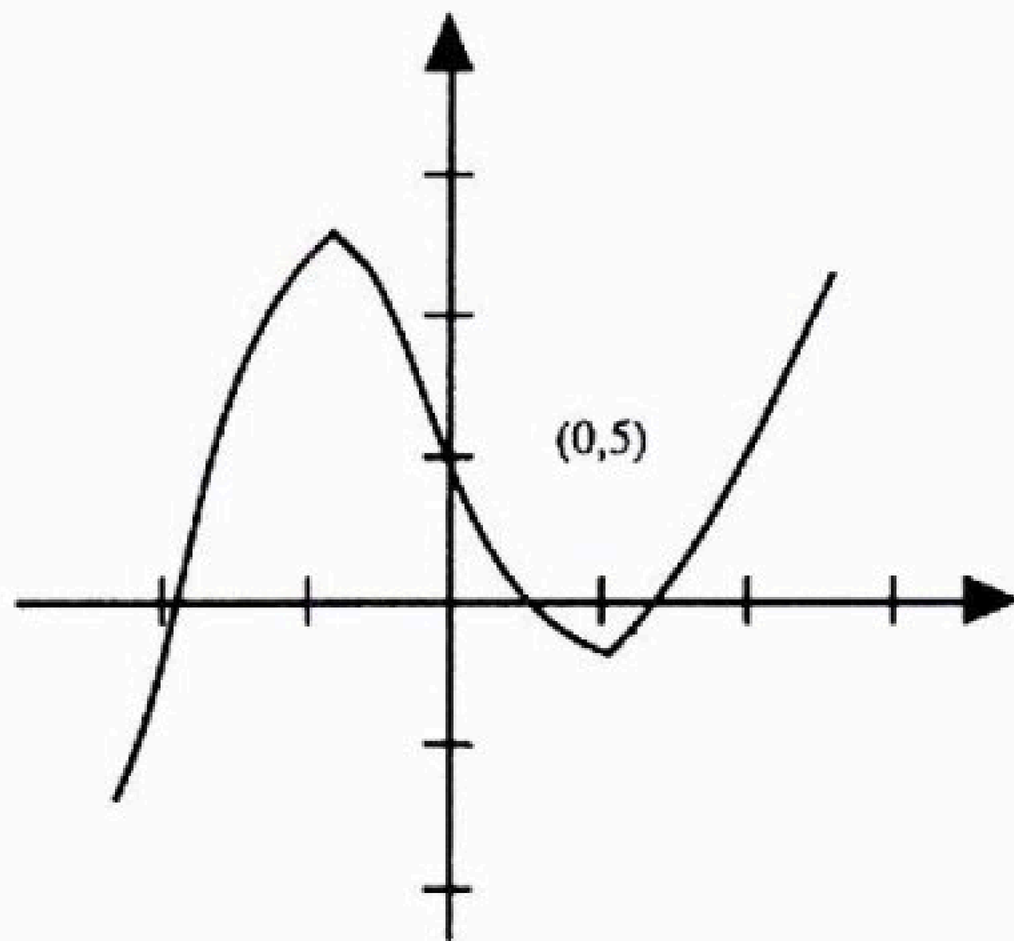
إن عناصر G تأخذ مجموعة جذور $q(x)$ إلى نفسها مما يجعلها تعرف تبديلات لـ $\alpha_1,\ldots,\alpha_p$. وبهذه الطريقة فإننا نقوم بإدخال G في S_p. إن التماثل الذاتي τ الذي وصف أعلاه هو المناقلة $(1,2)$ لأن $\tau(\alpha_1)=\alpha_2$ ، $\tau(\alpha_2)=\alpha_1$ ، $\tau(\alpha_i)=\alpha_i$ لكــل $i\geqslant 3$. ماذا عن العنصر σ في G المذكور أعلاه والذي رتبته تساوي p ؟ كعنصر في S_p رتبة σ هي p. ولكن العناصر الوحيدة التي رتبتها تساوي p في S_p هي الدورات التي طولها p. لذا فإن σ يجب أن يكون دورة طولها p.

إذن، فإن الزمرة G باعتبارها زمرة جزئية من S_p تحتوي على مناقلة ودورة طولها p. إنه لتمرين سهل نسبيا (انظر مسألة ٤) برهان أن أية مناقلة وأية دورة طولها p في S_p يولدان S_p. لذا فإن σ و τ يولدان S_p ، ولكنهما في G ، مما يجعل الزمرة المولَّدة منهما في G. إن محصلة كل هذا هي أن $G=S_p$. وبعبارة أخرى، إن زمرة جالوا لـ q(x) على Q هي حقًّا S_p مما يثبت المبرهنة.

إن المبرهنة تقدم لنا معيارًا عامًّا للحصول على S_p كزمرة جالوا على Q. الآن يجب أن نكوِّن كثيرة حدود من الدرجة p على حقل الأعداد النسبية بحيث تكون غير مختزلة على Q ولها بالضبط جذران غير حقيقيين. لأجل تكوين كثيرة حدود غير مختزلة نستعمل معيار ايزنشتاين (مبرهنة ٣-١٠-٢). وكي نجعل جذورها كلها حقيقية عدا اثنين منها نتصرف بمعاملات كثيرة الحدود وضمن مجال عمل معيار ايزنشتاين. هنا، نقدم التفاصيل في حالة p=5 دع $q(x)=2x^5-10x+5$. باستعمال معيار ايزنشتيان فإن q(x) غير مختزل على Q. نرسم

$$y=q(x)=2x^5-10x+5$$

باستخدام مبادىء التفاضل فإن للدالة المرسومة نهاية عظمى عند x=-1 ونهاية صغرى عند x=1 (انظر شكل ٥-٨-١). كما هو موضح في الرسم فإن المنحنى $y=q(x)=2x^5-10x+5$ يقطع محور x ثلاث مرات فقط. لذا فإن لـ q(x) بالضبط ثلاثة جذور حقيقية.



شكل (٥-٨-١)

وبناءً عليه فإن الجذرين الباقيين يجب أن يكونا عددين مركبين غير حقيقيين. إذن، $q(x)$ تحقق فرضيات مبرهنــة (٥ـ٨ـ١) مما يجعــل زمــرة جالـوا لها على Q تسـاوي S_5. باستخدام مبرهنة (٥ـ٧ـ٢) نستنتج أنه ليس ممكنا التعبير عن جذور $q(x)$ كتركيب من جذور نونية لأعداد نسبية.

مسـائــل

١ - في S_5 برهن على أن $(1\,2)$ و $(1\,2\,3\,4\,5)$ يولدان S_5.

٢ - في S_5 برهن على أن $(1\,2)$ و $(1\,3\,2\,4\,5)$ يولدان S_5.

٣ - إذا كان $p>2$ عددًا أوليًّا فبين أن $(1\,2)$ و $(1\,2 \ldots p-1\, p)$ يولدان S_p.

٤ - برهن على أن أية مناقلة وأية دورة طولها p في S_p يولدان S_p حيث p عدد أولي.

٥ - بين أن كثيرات الحدود التالية غير مختزلة على Q ولكل منها بالضبط جذران غير حقيقيين

(أ) $p(x)=x^3-3x-3$

(ب) $p(x)=x^5-6x+3$

(جـ) $p(x)=x^5+5x^4+10x^3+10x^2-x-2$

٦ - ما هي زمرة جالوا على Q لكثيرات الحدود في مسألة ٥؟

٧ - أنشيء كثيرة حدود من الدرجة 7 معاملاتها أعداد نسبية بحيث أن زمرة جالوا لها على Q هي S_7.

قراءة إضافية

Artin, E. *Galois Theory,* 2nd Ed. Notre Dame. Mathematical Lectures Number 2. Notre Dame Ind.: Notre Dame Press, 1966.

Kaplansky, Irving. *Fields and Rings,* 2nd Ed. Chicago: University of Chicago Press, 1972.

Pollard, H. *Theory of Algebraic Numbers,* Carus Monograph, Number 9. New York: John Wiley and Sons, 1950.

Van Der Waerden, B.L. *Modern Algebra, Vol. 1. New York:* Ungar Publishing Company, 1949.

Wiesner, L. *Theory of Equations.* New York: The Macmillan Company, 1938.

Siegal, C.L. *Transcendental Numbers,* Annals of Mathematics Studies Number 16. Princeton N.J.: Princeton University Press, 1949 and Milwood, N.Y.: Kraus Reprint Company, 1949.

Niven, I. *Irrational Numbers,* Carus Monograph Number II. New York: John Wiley and Sons, 1956.

مواضيع للمناقشة

Niven, I., "A simple proof of the irrationality of π". *Bulletin of the American Mathematical Society,* **53** (1947), page 509.

٦

التحويلات الخطية

● جبر التحويلات الخطية ● الجذور المميزة ● المصفوفات ● الصيغ القانونية: الصيغة المثلثية ● الصيغ القانونية: التحويلات المعدومة القوى ● الصيغ القانونية: تفريق الفضاء V (صيغة جوردان) ● الصيغ القانونية: الصيغة القانونية النسبية ● الأثر والمنقول ● المحددات ● التحويلات الهرميتية، الواحدية والناظمية ● الصيغ التربيعية الحقيقية.

لقد عرفنا في الفصل الرابع المجموعة Hom(V,W) بأنها تلك المجموعة التي تحتوي على جميع التشاكلات من V إلى W ، حيث V و W فضاءا متجهات على الحقل F نفسه. وفي الحقيقة، لقد عرفنا على Hom(V,W) عمليتي الجمع والضرب بالقياسيات (عناصر F) بطريقة تجعل من Hom(V,W) فضاء متجهات على F.

هناك حالة خاصة، لكنها ذات أهمية وذلك عندما V=W ، ذلك لأنه بالإضافة إلى عمليتي فضاء المتجهات يمكننا تعريف عملية الضرب لأي عنصرين بحيث تكون Hom(V,V) حلقة. إن Hom(V,V) من حيث كونها مزودة بهذه الميزة المزدوجة وهي ميزة فضاء المتجهات وميزة الحلقة لتكتسب بنية غنية جدا. إن هذه البنية وما يترتب عليها من نتائج لتضفي حيوية وبريقا على الموضوع مما يجعلها تبرر بشكل قوي استحداث فكرة المفهوم التجريدي لفضاء المتجهات.

إن اهتمامنا سيكون مركزا على Hom(V,V) ، حيث V هنا ليس أي فضاء متجهات اختياري بل إنه سيكون فضاء متجهات منته البعد على الحقل. إن نهائية

بعد V تفرض على $Hom(V,V)$ نتيجة هي أن كل عنصر من عناصره تحقق كثيرة حدود على F. إن هذه الحقيقية، لربما تخولنا أكثر من أية حقيقة أخرى الدخول مباشرة إلى $Hom(V,V)$ كما أنها تسمح لنا أن نسبر غور بنية $Hom(V,V)$ بكفاءة وعمق.

إن الموضوع الذي سنتناول دراسته غالبا ما يدعى **بالجبر الخطي** (Linear Algebra) والذي يشتمل على **نظرية المصفوفات** (Theory of Matrices). إن كون نتائجه تدخل في استخدام يومي في كل نواحي الرياضيات (وفي مواضيع أخرى) لهي عبارة لا مبالغة فيها.

هناك اعتقاد سائد ذلك هو أن الرياضيين يجدون متعة في عدم تطبيق مواضيعهم كما أنه يخيب أملهم عندما يقدم غيرهم على تطبيق نتائجهم. إن هذا الاعتقاد هراء محض. صحيح أن الرياضي لا يعتمد في مناقشاته على قابلية تطبيق نتائجه خارج نطاق الرياضيات ولكنه يعتمد، نوعا ما، على معيار رياضي جوهري غير ملموس لدى غيره. ومع ذلك فإنه صحيح، على حد سواء، إن معكوس ذلك خاطىء، بمعنى أن استخدام نتيجة ما لا ينقص من قيمتها الرياضية أبدا. مثال ذلك موضوع الجبر الخطي، إن هذا الموضوع رياضي مهم ومثير في حد ذاته. إنه، لربما، ذلك الموضوع من الرياضيات الذي يجد تطبيقات كثيرة في الفيزياء والكيمياء والاقتصاد، ليس في هذه المواضيع فحسب، بل في الحقيقة في كل علم.

(٦-١) جبر التحويلات الخطية

ليكن V فضاء متجهات على الحقل F. ولتكن $Hom(V,V)$ هي مجموعة جميع تشاكلات فضاء المتجهات من V إلى نفسه. لقد أثبتنا في البند (٤-٣) أن $Hom(V,V)$ فضاء متجهات على الحقل F. كما أنه لأي تشاكلين $T_1,T_2 \in Hom(V,V)$ يكون T_1+T_2 معرفا بالقاعدة $v(T_1+T_2)=vT_1+vT_2$ وذلك لكل $v \in V$، كما أنه لأي قياسي $\alpha \in F$ يكون αT_1 معرفا بالقاعدة $v(\alpha T_1)=\alpha(vT_1)$. إن للتعبير $(vT_1)T_2$ معنى وذلك لأي تشاكلين T_1 و T_2 في $Hom(V,V)$ ولأي v في V. ذلك لأن $vT_1 \in V$. إننا نعرف T_1T_2 بالقاعدة $vT_1T_2=(vT_1)T_2$ وذلك بالطريقة نفسها التي عملناها للتطبيقات من أية مجموعة إلى نفسها وذلك لأي $v \in V$. إننا ندعي الآن أن $T_1T_2 \in Hom(V,V)$،

لبرهان ذلك يجب علينا أن نثبت أنه لأي قياسيين α و β في F ولجميع $u,v\in V$ يكون

$$(\alpha u+\beta v)T_1T_2=\alpha(u(T_1T_2))+\beta(v(T_1T_2))$$

الآن :

$$\begin{aligned}(\alpha u+\beta v)(T_1T_2) &= ((\alpha u+\beta v)T_1)T_2\\ &=(\alpha(uT_1)+\beta(vT_1))T_2\\ &=\alpha(uT_1)T_2+\beta(vT_1)T_2\\ &=\alpha(u(T_1T_2))+\beta(v(T_1T_2))\end{aligned}$$

إن براهين الخواص الآتية للضرب في $Hom(V,V)$ متروكة كتمرين .

١) $(T_1+T_2)T_3=T_1T_3+T_2T_3$

٢) $T_3(T_1+T_2)=T_3T_1+T_3T_2$

٣) $T_1(T_2T_3)=(T_1T_2)T_3$

٤) $\alpha(T_1T_2)=(\alpha T_1)T_2=T_1(\alpha T_2)$

وذلك لكل $T_1,T_2,T_3\in Hom(V,V)$ ولكل $\alpha\in F$.

لاحظ أن الخواص الثلاث الأولى الواردة أعلاه هي تلك الخواص المطلوبة لكي تجعل من $Hom(V,V)$ حلقة تجميعية، كما أن الخاصة الرابعة منها تربط بين كون $Hom(V,V)$ فضاء متجهات وكونه حلقة .

كذلك، لاحظ أنه يوجد عنصر I في $Hom(V,V)$ معرف بالقاعدة $vI=v$ لكل $v\in V$ ويحقق الخاصة $TI=IT=T$ لكل $T\in Hom(V,V)$ وبهذا يكون $Hom(V,V)$ حلقة بعنصر وحدة. وفضلا عن ذلك إذا وضعنا $T_2=I$ في الخاصة الرابعة فإنا نحصل على $\alpha T_1=T_1(\alpha I)$ وحيث إن $(\alpha I)T_1=\alpha(IT_1)=\alpha T_1$ لذلك نجد أن $(\alpha I)T_1=T_1(\alpha I)$ وذلك لكل $T_1\in Hom(V,V)$ ، أي أن αI يتبادل مع كل عنصر في $Hom(V,V)$ وسنكتب، دائما، في المستقبل αI على أنه α.

تعريف

يقال إن الحلقة التجميعية A هي جبر (Algebra) على الحقل F إذا كانت A فضاء متجهات على F وكان بالإضافة إلى ذلك $\alpha(ab)=(\alpha a)b=a(\alpha b)$ لكل $a,b\in A$ ولكل $\alpha\in F$.

إن تشاكلات وتماثلات ومثاليات الجبريات معرفة كما في الحلقات مع إضافة شرط محافظتها على بناء فضاء المتجهات.

إن الملاحظات الواردة آنفا تدل على أن Hom(V,V) هو جبر على F ولتسهيل الاصطلاحات، سنكتب من الآن فصاعدا Hom(V,V) على أنه A(V) ومتى ما أردنا التأكيد على دور الحقل F فإننا سنكتبه بالصيغة $A_F(V)$.

تعريف

إن التحويل الخطي على فضاء المتجهات V على الحقل F هو عنصر من $A_F(V)$.

سنشير، أحيانا، إلى A(V) على أنه **حلقة** أو **جبر التحويلات الخطية على V**. إننا نستطيع إثبات نظيرة مبرهنة كيلي للزمر وذلك بالنسبة لأي جبر A بعنصر الوحدة على الحقل F وذلك في التمهيدية الآتية.

تمهيدية (٦-١-١)

إذا كان A جبرا بعنصر وحدة على الحقل F فإن A يماثل جبرًا جزئيًا من A(V)، حيث V فضاء متجهات ما على الحقل F.

البرهان

لما كان A جبرًا على F لذلك فإنه يجب أن يكون فضاء متجهات على F ولهذا سنضع A = V لكي نبرهن التمهيدية.

إذا كان $a \in A$ فإننا نعرف $T_a: A \to A$ كما يلي $vT_a = va$ لكل $a \in A$. إن T_a تحويل خطي على V(=A) وذلك لأنه من قانون التوزيع على اليمين نجد

$$(v_1+v_2)\, T_a = (v_1+v_2)a = v_1a + v_2a = v_1T_a + v_2T_a$$

وحيث إن A جبر، فإنه يكون

$$(\alpha v)T_a = (\alpha v)a = \alpha(va) = \alpha(vT_a)$$

وذلك لأي $a \in A$ ولأي $\alpha \in F$. أي أن T_a فعلا تحويل خطي على A.

لنعتبر التطبيق $\psi: A \to A(V)$ المعرف بالقاعدة $a\psi = T_a$ لكل $a \in A$. إن ψ تماثل من A إلى $A(V)$ ولإثبات ذلك نفرض أن $a,b \in A$ وأن $\alpha,\beta \in F$ ، عندئذ

$$vT_{\alpha a+\beta b} = v(\alpha a+\beta b) = \alpha(va) + \beta(vb)$$

وذلك لكل $v \in A$. ووفقاً لقانون التوزيع من اليسار وكون A جبر على F نجد أن ذلك يساوي :

$$\alpha(vT_a) + \beta(vT_b) = v(\alpha T_a + \beta T_b)$$

وذلك لأن كلا من T_a و T_b تحويل خطي وبالتالي فإن $T_{\alpha a+\beta b} = \alpha T_a + \beta T_b$. ومن ثم فإن ψ هو تشاكل فضاء متجهات من A إلى $A(V)$. بعد ذلك، نحسب vT_{ab} حيث $a,b \in A$ ، حيث نجد

$$vT_{ab} = v(ab) = (va)b = (vT_a)T_b = v(T_aT_b)$$

(لقد استخدمنا قانون التجميع في هذه الحسابات) وهذا يقتضي أن $T_{ab} = T_aT_b$. وبهذه الطريقة نجد أن ψ هو تشاكل حلقة من A إلى $A(V)$. إلى هنا نكون قد برهنا على أن ψ هو تشاكل من A ، باعتباره جبرا، إلى $A(V)$ وكل ما بقي لدينا هو تحديد نواة ψ. لنفرض أن العنصر $a \in A$ ينتمي إلى نواة ψ عندئذ $a\psi = 0$ ، أي أن $T_a = 0$ وبالتالي فإن $vT_a = 0$ لكل $v \in A$. الآن، إن $V = A$ كما أن A يحتوي على عنصر وحدة هو e ولذلك $eT_a = 0$. وفضلا عن ذلك فإن $0 = eT_a = ea = a$. وبذلك نكون قد أثبتنا أن $a = 0$ أي أن النواة تتكون فقط من العنصر 0 مما يقتضي أن ψ تماثل من A إلى $A(V)$ وبهذا ينتهي برهان التمهيدية.

إن التمهيدية تحدد الدور الهام الذي تلعبه الجبريات $A(V)$ إذ أنه في هذه الجبريات يمكن أن نجد صورة مماثلة لأي جبر.

لنفرض أن A جبر بعنصر وحدة على الحقل F وليكن $p(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ كثيرة حدود في $F[x]$. فإذا كان $a \in A$ فإن $p(a)$ يعني العنصر $\alpha_0 e + \alpha_1 a + \ldots + \alpha_n a^n$ في A. وإذا كان $p(a) = 0$ فإننا نقول عندئذ إن a *يحقق* $p(x)$.

تمهيدية (٦-١-٢)

لنفرض أن A جبر بعنصر وحدة على F وأن بعد A على F هو m ، عندئذ كل عنصر في A يحقق كثيرة حدود في $F[x]$ درجتها على الأكثر هي m.

البرهان

ليكن e هو عنصر الوحدة في A فإذا كان $a \in A$ فلنعتبر العناصر $e,a,a^2,\ldots,a^m$ في A التي عددها m+1. وحيث إن بعد A على F هو m واستنادا إلى تمهيدية (٤-٢-٤) فإن العناصر $e,a,a^2,\ldots,a^m$ يجب أن تكون مرتبطة خطيا على F إذ أن عددها هو m+1. وبعبارة أخرى، توجد عناصر $\alpha_0,\alpha_1,\ldots,\alpha_m$ في F ليست كلها أصفارًا بحيث يكون $\alpha_0 e+\alpha_1 a+\ldots+\alpha_m a^m=0$ وعندئذ فإن a يحقق كثيرة الحدود غير التافهة $q(x)=\alpha_0+\alpha_1 x+\ldots+\alpha_m x^m$ التي درجتها على الأكثر هي m في F[x].

إذا كان V فضاء متجهات منتهي البعد على F وكان بعده هو n فإنه استنادا إلى النتيجة الأولى للمبرهنة (٤-٣-١) يكون بعد A(V) على F هو n^2. وحيث إن A جبر على F ، لذا فإننا نستطيع تطبيق تمهيدية (٦-١-٢) عليه لنجد أن كل عنصر من A(V) يحقق كثيرة حدود على F درجتها هي على الأكثر n^2. إن لهذه الحقيقة أهمية جوهرية في جميع ما سيتبع ولذلك فإننا ندونها على الصيغة الآتية.

مبرهنة (٦-١-١)

إذا كان V فضاء متجهات على F وكان بعده n وإذا كان T هو أي عنصر من A(V) فإنه توجد كثيرة حدود غير تافهة $q(x) \in F[x]$ درجتها على الأكثر n^2 بحيث تكون $q(T)=0$.

سنرى فيما بعد أنه يمكننا أن نقول الشيء الكثير عن درجة q(x) وفي الحقيقة سنكون قادرين على أن نجد كثيرة حدود q(x) بحيث تكون درجتها على الأكثر n. إن هذه الحقيقة ليست إلا مبرهنة شهيرة في هذا الموضوع هي تلك المعروفة بمبرهنة **كيلي هاملتون** (Cayley-Hamilton). ولكننا في الوقت الحاضر يمكن أن نستمر دون حاجة إلى تقدير دقيق لدرجة q(x) وكل ما نحتاجه وجود كثيرة حدود مناسبة.

لما كان لكل $T \in A(V)$ ، حيث V فضاء متجهات منتهي البعد، توجد كثيرة حدود ما q (x) بحيث يكون $q(T) = 0$. إنه بالإمكان إيجاد كثيرة حدود من درجة دنيا هي p (x) في F[x] تتمتع بهذه الخاصة. ونطلق على كثيرة الحدود p(x) **كثيرة الحدود الدنيا (minimal polynomial)** للتحويل الخطي T على F. وإذا كان T يحقق كثيرة حدود ما هي h(x) فإن $p(x)|h(x)$.

تعريف

يقال إن للعنصر $T \epsilon A(V)$ ***معكوس أيمن*** *(right inverse) إذا وجد $S \epsilon A(V)$ بحيث يكون $TS=1$ (إن 1 هنا يرمز إلى عنصر الوحدة في A(V)).*

وبالمثل تعريف **المعكوس الأيسر** (left inverse) وذلك إذا وجد $U \epsilon A(V)$ بحيث يكون $UT=1$. وإذا كان لـ T معكوس أيمن وأيسر وكان $TS=UT=1$ فإن من السهل إثبات أن $S=U$ وأن S وحيد ونترك لك ذلك كتمرين.

تعريف

يقال إن للعنصر $T \epsilon A(V)$ ***معكوس*** *(inverse) أو أنه* ***منتظم*** *(regular) وذلك إذا وجد له معكوس أيمن وأيسر، بمعنى أنه إذا وجد عنصر $S \epsilon A(V)$ بحيث يكون $ST=TS=1$ وسنكتب S على الشكل T^{-1}.*

يقال عن العنصر الذي ليس منتظما في A(V) إنه **شاذ** (singular). إنه من الممكن تماما لعنصر من A(V) أن يوجد له معكوس أيمن دون أن يكون منتظما.
مثال ذلك، ليكن F هو حقل الأعداد الحقيقية وليكن V هو F[x] ، أي مجموعة كثيرات الحدود في المتغير x على F وليكن $S \epsilon V$ معرفا كما يلي:

$$q(x)S = \frac{d}{dx} q(x)$$

وليكن T معرفا كما يلي

$$q(x)T = {}_1\int^x q(x)\, dx$$

عندئذ $ST\neq 1$ بينما $TS=1$ وكما سنرى بعد قليل، *أنه إذا كان V منتهي البعد على F* فإنه يوجد معكوس للعنصر الذي له معكوس أيمن في $A(V)$.

مبرهنة (٦-١-٢)

إذا كان V منتهي البعد على F فإنه يوجد معكوس للعنصر $T\in A(V)$ إذا وفقط إذا كان الحد الثابت من كثيرة الحدود الدنيا لـ T ليس صفرا.

البرهان

لتكن $p(x)=\alpha_0+\alpha_1 x+\ldots+\alpha_k x^k$ و $\alpha_k\neq 0$ ، هي كثيرة الحدود الدنيا لـ T على F. فإذا كان $\alpha_0\neq 0$ وحيث إن

$$0=p(T)=\alpha_k T^k+\alpha_{k-1}T^{k-1}+\ldots+\alpha_1 T+\alpha_0$$

فإننا نجد:

$$1=T\left(-\frac{1}{\alpha_0}(\alpha_k T^{k-1}+\alpha_{k-1}T^{k-2}+\ldots+\alpha_1)\right)$$

$$=\left(-\frac{1}{\alpha_0}(\alpha_k T^{k-1}+\ldots+\alpha_1)\right)T$$

وبناء عليه فإن

$$S=-\frac{1}{\alpha_0}(\alpha_k T^{k-1}+\ldots+\alpha_1)$$

هو معكوس T ومن ثم فإنه يوجد لـ T معكوس.

ومن ناحية أخرى، لنفرض أنه يوجد معكوس لـ T وأن $\alpha_0=0$ ومن ثم فإن

$$0=\alpha_1 T+\alpha_2 T^2+\ldots+\alpha_k T^k=(\alpha_1+\alpha_2 T+\ldots+\alpha_k T^{k-1})T$$

بضرب هذه العلاقة من اليمين بـ T^{-1} نحصل على:

$$\alpha_1+\alpha_2 T+\ldots+\alpha_k T^{k-1}=0$$

$$q(x)=\alpha_1+\alpha_2 x+\ldots+\alpha_k x^{k-1}$$

في $F[x]$. وحيث إن درجة $q(x)$ أقل من درجة $p(x)$ وهذا غير ممكن لذلك يكون $\alpha_0 \neq 0$ وبذلك يتم إثبات المبرهنة.

نتيجة (١)

إذا كان V منتهي البعد على F وكان يوجد معكوس لـ $T \in A(V)$ فإنه يمكن التعبير عن T^{-1} على هيئة كثير حدود في T على F.

البرهان

لما كان يوجد معكوس لـ T ، لذلك فإنه وفقًا للمبرهنة نجد أن:

$$\alpha_0 \neq 0 \, , \, \alpha_0 + \alpha_1 T + \ldots + \alpha_k T^k = 0$$

ولكن عندئذ:

$$T^{-1} = -\frac{1}{\alpha_0}\left(\alpha_1 + \alpha_2 T + \ldots + \alpha_k T^{k-1}\right)$$

نتيجة (٢)

إذا كان V منتهي البعد على F وكان $T \in A(V)$ شاذًا فإنه يوجد $S \neq 0$ في $A(V)$ بحيث يكون $ST = TS = 0$

البرهان

لما كان T غير منتظم لذا فإن الحد الثابت في كثيرة حدودها الدنيا يجب أن يكون صفـرا. أي أن $p(x) = \alpha_1 x + \ldots + \alpha_k x^k$ ومـن ثم فإن $0 = \alpha_1 T + \ldots + \alpha_k T^k$. إذا كان $S = \alpha_1 + \ldots + \alpha_k T^{k-1}$ فإن $S \neq 0$ (لأن درجة $\alpha_1 + \ldots + \alpha_k x^{k-1}$ أقل من درجة $p(x)$) كذلك فإن $ST = TS = 0$.

نتيجة (٣)

إذا كان V منتهي البعد على F ووُجِد معكوس أيمن لـT فإنه يوجد معكوس لـT .

البرهان

ليكن $TU=1$. لو كان T شاذًّا فإنه يوجد S و $S\neq 0$ بحيث إن $ST=0$.
ومع ذلك فإن

$$0=(ST)U=S(TU)=S1=S\neq 0$$

وهذا تناقض وبالتالي فإن T منتظم.

الآن نود تحويل المعلومات الموجودة في مبرهنة ٦ـ١ـ٢ ونتائجها من $A(V)$ إلى تأثير T على V. إن النتيجة الأساسية بهذا الخصوص هي.

مبرهنة (٦ـ١ـ٣)

إذا كان V منتهي البعد على F فإن $T\in A(V)$ يكون شاذًّا إذا وفقط إذا وجد $v\in V$، $v\neq 0$ بحيث يكون $vT=0$.

البرهان

من نتيجة (٢) لمبرهنة (٦ـ١ـ٢) يكون T شاذا إذا وفقط إذا وجد $S\neq 0$ في $A(V)$ بحيث يكون $ST=TS=0$. وحيث إن $S\neq 0$، لذلك فإنه يوجد عنصر $w\in V$ بحيث يكون $wS\neq 0$.

ليكن $v=wS$، عندئذ

$$vT=(wS)T=w(ST)=w0=0$$

وبذلك نكون قد حصلنا على متجه غير صفري v في V الذي ينعدم بواسطة T. وبالعكس، إذا كان $vT\neq 0$ حيث $v=0$ فإننا نترك برهان أنه لا يوجد معكوس لـ T كتمرين.

نحن لا نزال بصدد البحث عن مميز آخر لشذوذ أو انتظام تحويل خطي بدلالة تأثيره الكلي على V.

تعريف

إذا كان $T\in A(V)$ فإننا نعرف مدى T (range) ، أي VT كما يلي

$$VT=\{vT/v\in V\}$$

يمكن إثبات أن مدى T هو فضاء جزئي من V . إنه يتكون من صور عناصر V بواسطة T. لاحظ أن مدى T هو كل V إذا وفقط إذا كان T غامرًا.

مبرهنة (٦-١-٤)

إذا كان V منتهي البعد على F فإن $T\in A(V)$ يكون منتظما إذا وفقط إذا كان T يطبق V على نفسه.

البرهان

كما هو الحال غالبا، فإن أحد اتجاهي هذه المبرهنة يكاد يكون تافهًا ذلك هو أنه إذا كان T منتظما فإن $v=(vT^{-1})T$ حيث $v\in V$ ومن ثم فإن $VT=V$ ، أي أن T غامر.

ومن ناحية أخرى، لنفرض أن T ليس منتظما ومن ثم يجب أن نثبت أن T ليس غامرًا. الآن، لما كان T شاذًا فإنه استنادًا إلى مبرهنة (٦-١-٣) يوجد متجه $0\neq v_1\in V$ في V بحيث يكون $v_1T=0$. استناذا إلى تمهيدية (٤-٢-٥) فإنه يمكن توسيع v_1 إلى أساس $v_1,v_2,\dots,v_n$ لـ V. وبالتالي فإن كل متجه في VT هو تركيب خطي للعناصر $w_1=v_1T, w_2=v_2T,\dots, w_n=v_nT$ ولما كان $w_1=0$ وأيضا لما كان VT مولدا بعناصر عددها $n-1$ هي $w_2,\dots,w_n$ فإننا نجد أن :

$$\dim VT=n-1<n=\dim V$$

وعندئذ فإن VT مختلف عن V الأمر الذي يعني أن T ليس غامرا.

إن مبرهنة (٦-١-٤) توضح لنا أنه يمكن تمييز العناصر المنتظمة من الشاذة في حالة فضاءات المتجهات المنتهية البعد وذلك حسبما يكون التحويل الخطي غامرًا أم لا .

فإذا كان $T\in A(V)$ فإنه يمكننا أن نعبر عن ذلك بقولنا إن T منتظم إذا وفقط إذا كان $\dim VT=\dim V$. إن هذا يقرر لنا أنه يمكن استخدام $\dim(VT)$ ليس فقط كأداة لاختبار الانتظام ولكن كمقياس لدرجة الشذوذ (أو لنقص الانتظام) لعنصر T من $A(V)$.

تعريف

إذا كان V منتهي البعد على F فإن مرتبة (rank) T هي بعد VT على F ، حيث VT هو صورة T.

سنرمز لمرتبة T بالرمز $r(T)$. فإن كان $r(T)=\dim V$ فإن T منتظم (ومن ثم فإنه ليس شاذًا على الإطلاق). ومن ناحية أخرى إذا كان $r(T)=0$ فإن $T=0$ الأمر الذي يجعل T شاذًا إلى أقصى حد. إن المرتبة، باعتبارها دالة على $A(V)$ هي دالة مهمة جدا وفيما يلي ندرس بعض خواصها.

تمهيدية (٦-١-٣)

إذا كان V منتهي البعد على F فإنه لأي $S,T\in A(V)$ يكون

١) $r(ST)\leq r(T)$

٢) $r(TS)\leq r(T)$ ، (ومن ثم فإن $r(ST)\leq \min\{r(T),r(S)\}$)

٣) $r(ST)=r(TS)=r(T)$ وذلك لعنصر منتظم S من $A(V)$.

البرهان

نبدأ بالترتيب

١) لما كان $VS\subset V$ و $V(ST)=(VS)T\subset VT$ ، لذا فإنه وفقا لتمهيدية (٤-٢-٦) يكون $\dim(V(ST))\leq \dim VT$ ، أي أن $r(ST)\leq r(T)$.

٢) لنفرض أن $r(T)=m$ عندئذ فإن أساس VT يتكون من عناصر عددها m هي $w_1,w_2,\ldots,w_m$ ولكن $(VT)S$ عندئذ يكون مولدًا بالعناصر $w_1S,\ldots,w_mS$ ومن ثم فإن بعده على الأكثر يساوي m ولما كان:

$$r(TS)=\dim(V(TS))=\dim((VT)S)\leqslant m=\dim VT=r(T)$$

فإنه بذلك يتم برهان (٢).

٣) إذا كان S منتظما فإن $VS=V$ ومن ثم فإن $V(ST)=(VS)T=VT$ وبالتالي فإن:

$$r(ST)=\dim(V(ST))=\dim VT=r(T)$$

ومن ناحية أخرى، إذا كانت العناصر $w_1,\ldots,w_m$ هي أساس V فإن انتظام S يقتضي أن تكون العناصر $w_1S,\ldots,w_mS$ مستقلة خطيا (برهن ذلك).

وحيث إن هذه العناصر تولد $V(TS)$ فإنها تكون أساسا لـ $V(TS)$ وعندئذ:

$$r(TS)=\dim(V(TS))=\dim VT=r(T)$$

نتيجة

إذا كان $T\in A(V)$ وكان $S\in A(V)$ منتظما فإن $r(T)=r(STS^{-1})$

البرهان

من الجزء الثالث من التمهيدية السابقة نجد

$$r(STS^{-1})=r(S(TS^{-1}))=r((TS^{-1})S)=r(T)$$

مسائل

افرض أن V فضاء متجهات منتهي البعد على الحقل F وذلك في جميع المسائل ما لم ينص على خلاف ذلك.

١ - أثبت أن $S\in A(V)$ يكون منتظما إذا وفقط إذا أنه مهما كانت العناصر $v_1,\ldots,v_n\in V$ مستقلة خطيا فإن $v_1S,v_2S,\ldots,v_nS$ مستقلة خطيا أيضا.

٢ - برهن على أن $T\in A(V)$ يتعين تماما وذلك بمعرفة تأثيره على أساس V.

٣ - أثبت تمهيدية (٦-١-١) حتى ولو كان A لا يحتوي على عنصر وحدة.

٤ - إذا كان A هو حقل الأعداد المركبة و F هو حقل الأعداد الحقيقية فإن A جبر بعده 2 على F وإذا كان $a=\alpha+\beta i\in A$. فاحسب تأثير T_a على أساس A على F (انظر تمهيدية ٦-١-١).

٥ - إذا كان بعد V على F يساوي 2 وكان $A=A(V)$. فاكتب أساس A على F ثم احسب T_a لكل عنصر a في الأساس.

٦ - إذا كان $\dim_F V>1$. فأثبت أن $A(V)$ ليس إبداليًّا.

٧ - لتكن $Z=\{T\in A(V)|ST=TS:A(V)$ لكل S في $\}$ مجموعة في $A(V)$. أثبت أن Z تتكون من حاصل ضرب عنصر الوحدة في $A(V)$ بعناصر من F.

٨* - إذا كان $\dim_F V>1$. فأثبت أن $A(V)$ لا يحتوي على مثاليات ثنائية الجانب سوى (0) و $A(V)$.

٩** - أثبت أن استنتاج مسألة (٨) يكون غير صحيح إذا لم يكن V منتهي البعد على F.

١٠ - إذا كان V فضاء متجهات ما على F وكان لـ $T\in A(V)$ معكوس أيمن وأيسر. فأثبت تساوي المعكوس الأيمن مع المعكوس الأيسر ومن هذا أثبت أن معكوس T وحيد.

١١ - إذا كان V فضاء متجهات ما على F وكان يوجد لـ $T\in A(V)$ معكوس أيمن وحيد. فأثبت أنه يوجد لـ T معكوس.

١٢ - أثبت أن العناصر المنتظمة في $A(V)$ تشكل زمرة.

١٣ - إذا كان F هو حقل الأعداد الصحيحة قياس 2 وإذا كان بعد V على F يساوي 2. فاحسب زمرة العناصر المنتظمة في $A(V)$ ثم أثبت أن هذه الزمرة تماثل S_3، أي زمرة التناظر من الدرجة الثالثة.

١٤* - إذا كان F حقلا منتهيا مكونا من عناصر عددها q. فاحسب رتبة زمرة العناصر المنتظمة في $A(V)$، حيث إن بعد V على F يساوي 2.

١٥* - حل المسألة (١٤) في حالة كون بعد V على F يساوي n.

١٦* - إذا كان V منتهي البعد. فأثبت أن كل عنصر من $A(V)$ يمكن كتابته على شكل مجموع عناصر منتظمة.

١٧ - يقال عن العنصر $E\in A(V)$ إنه **متساوي القوى** (idempotent) إذا كان $E^2=E$. فإذا كان $E\in A(V)$ متساوي القوى. فأثبت أن $V=V_0\oplus V_1$ حيث $v_0E=0$ لكل $v_0\in V_0$ و $v_1E=v_1$ لكل $v_1\in V_1$.

١٨ - إذا كان $T\in A_F(V)$ وكان مميز F لا يساوي 2 وكان $T^3=T$. فأثبت أن

$V=V_0\oplus V_1\oplus V_2$ حيث

أ) $v_0\in V_0$ يقتضي أن $v_0T=0$

ب) $v_1\in V_1$ يقتضي أن $v_1T=v_1$

جـ) $v_2\in V_2$ يقتضي أن $v_2T=-v_2$

١٩* ـ إذا كان V منتهي البعد وكان $0\neq T\in A(V)$. فأثبت أنه يوجد عنصر $S\in A(V)$ بحيث يكون $E=TS\neq 0$ عنصرا متساوي القوى.

٢٠ ـ يقال عن العنصر $T\in A(V)$ إنه **معدوم القوى** (nilpotent) إذا كان $T^m=0$ حيث m عدد ما، فإذا كان T معدوم القوى وكان $vT=\alpha v$ ، حيث $v\neq 0$ عنصر ما في V و $\alpha\in F$ فأثبت أن $\alpha=0$.

٢١ ـ إذا كان T معدوم القوى. فأثبت أن $\alpha_0+\alpha_1T+\alpha_2T^2+\ldots+\alpha_kT^k$ منتظم شريطة أن يكون $\alpha_0\neq 0$.

٢٢ ـ إذا كان A جبرا منتهي البعد على F وكان $a\in A$. فأثبت أنه لعدد صحيح ما k ، $k>0$ ولكثيرة حدود ما $p(x)\in F[x]$ يكون $a^k=a^{k+1}p(a)$.

٢٣ ـ أثبت، باستخدام المسألة (٢٢)، أنه إذا كان $a\in A$ فإنه توجد كثيرة حدود $q(x)\in F[x]$ بحيث يكون $a^k=a^{2k}q(a)$.

٢٤ ـ أثبت، باستخدام المسألة (٢٣)، أنه إذا كان $a\in A$ فإن a إما أن يكون معدوم القوى أو أنه يوجد عنصر $0\neq b\in A$ من الشكل $b=ah(a)$ ، حيث $h(x)\in F[x]$ ، بحيث يكون $b^2=b$.

٢٥ ـ إذا كان A جبرا على F (ليس ضروريا أن يكون منتهي البعد) وإذا كان a^2-a معدوم القوى، حيث $a\in A$. فأثبت أن a إما أن يكون معدوم القوى أو أنه يوجد عنصر b من الصيغة $b=ah(a)\neq 0$ حيث $h(x)\in F[x]$ ، بحيث يكون $b^2=b$.

٢٦* ـ إذا كان $0\in T=A(V)$ شاذًا. فأثبت أنه يوجد عنصر $S\in A(V)$ بحيث يكون $TS=0$ ولكن $ST\neq 0$.

٢٧ ـ لنفرض أن بعد V على F يساوي 2 وأن أساس V هو v_1,v_2 ولنفرض أن $T\in A(V)$ بحيث إن $v_1T=\alpha v_1+\beta v_2$ و $v_2T=\gamma v_1+\delta v_2$ حيث $\alpha,\beta,\gamma,\delta\in F$. أوجد كثيرة حدود غير صفرية في $F[x]$ درجتها تساوي 2 محققة من قبل T.

٢٨ - إذا كان بعد V على F يساوي 3 وكان أساس V هو v_1,v_2,v_3 وكان $T\in A(V)$ بحيث أن $v_i T = a_{i_1} v_1 + a_{i_2} v_2 + a_{i_3} v_3$ ، $i=1,2,3$ ولكل $a_{i_j}\in F$. أوجد كثيرة حدود درجتها تساوي 3 محققة من قبل T.

٢٩ - ليكن بعد V على F يساوي n وليكن أساس V هو $v_1,\ldots,v_n$ ولنفرض أن $T\in A(V)$ بحيث يكون:

$$v_1T=v_2, v_2T=v_3,\ldots,v_{n-1}T=v_n,\ \ v_nT=-\alpha_n v_1-\alpha_{n-1}v_2-\ldots-\alpha_1 v_n$$

حيث $\alpha_1,\ldots,\alpha_n\in F$. فأثبت أن T يحقق كثيرة حدود

$p(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n$ على F.

٣٠ إذا كان $T\in A(V)$ يحقق كثيرة الحدود $q(x)\in F[x]$. فأثبت أن STS^{-1} يحقق أيضا $q(x)$ حيث $S\in A(V)$ عنصر منتظم.

٣١ - (أ) إذا كان F هو حقل الأعداد النسبية وكان بعد V على F يساوي 3 وكان v_1,v_2,v_3 هو أساس V. فاحسب مرتبة $T\in A(V)$ المعرف بالقاعدة

$$v_1T=v_1-v_2$$
$$v_2T=v_1+v_3$$
$$v_3T=v_2+v_3$$

(ب) أوجد متجها $v\in V$, $v\neq 0$ بحيث يكون $vT=0$

٣٢ - برهن على أن مدى T و $U=\{v\in V|vT=0\}$ هما فضاءان جزئيان من V.

٣٣ - إذا كان $T\in A(V)$ وكان $V_0=\{v\in V|vT^k=0\}$ حيث k عدد ما. أثبت أن V_0 فضاء جزئي وأنه إذا كان $vT^m\in V_0$ فإن $v\in V_0$.

٣٤ - أثبت أن كثيرة الحدود الدنيا لـ T على F تقسم جميع كثيرات الحدود المختلفة المحققة من قبل T على F.

٣٥*- إذا كان $n(T)$ هو بعد U الوارد في المسألة (٣٢). فأثبت أن $r(T)+n(T)=\dim V$.

(٦-٢) الجـذور المميزة

سنقصر اهتمامنا في بقية الفصل على التحويلات الخطية على فضاءات المتجهات المنتهية البعد وعليه فإنه من الآن فصاعدا، *سيكون V دائما فضاء متجهات منتهي البعد على الحقل F* .

إن الجبر $A(V)$ يحتوي على عنصر وحدة وللسهولة سنرمز له بالرمز 1 ، كما أن الرمز $\lambda-T$ ، حيث $T\in A(V)$ و $\lambda\in F$ يعني بالنسبة لنا $\lambda 1-T$.

تعريف

*إذا كان $T\in A(V)$ فإن $\lambda\in F$ يدعى **جذرا مميـزا** (characteristic root) أو **قيمـة واقعية** (Eigenvalue) لـ T إذا كان $\lambda-T$ شاذًا .*

نود، فيما يلي، تمييز خاصية كون عنصر من F جذرًا مميزًا وذلك بمعرفة سلوك T على V.

مبرهنة (٦-٢-١)

يكون العنصر $\lambda\in F$ جذرا مميزا لـ $T\in A(V)$ إذا وفقط إذا كان $vT=\lambda v$ ، حيث $0\neq v\in V$

البرهان

إذا كان λ جذرا مميزا لـ T فإن $\lambda-T$ شاذ ومن ثم، ومن مبرهنة (٦-١-٣)، يوجد متجه $0\neq v\in V$ بحيث يكون $v(\lambda-T)=0$ وعندئذ فإن $\lambda v=vT$.

ومن ناحية أخرى، إذا كان $vT=\lambda v$ ، حيث $0\neq v\in V$ ، فإن $v(\lambda-T)=0$ وبالتالي ووفقا لمبرهنة (٦-١-٣) يجب أن يكون $\lambda-T$ شاذًا، أي أن λ هو جذر مميز لـ T.

تمهيدية (٦-٢-١)

إذا كان $\lambda\in F$ جذرا مميزا لـ $T\in A(V)$ فإنه لأي كثيرة حدود $q(x)\in F[x]$ يكون $q(\lambda)$ جذرًا مميزًا لـ $q(T)$.

البرهان

لنفرض أن $\lambda\in F$ جذرا مميزا لـ T. عندئذ، استنادا إلى مبرهنة (٦-٢-١) يوجد متجه غير صفري v في V بحيث يكون $vT=\lambda v$. ماذا يمكن أن نقول عن vT^2 ؟

الآن $vT^2=(\lambda v)T=\lambda(vT)=\lambda(\lambda v)=\lambda^2 v$. بالاستمرار بهذه الطريقة نجد أن $vT^k=\lambda^k v$ وذلك لجميع الأعداد الصحيحة الموجبة k. إذا كان $q(x)=a_0x^m+a_1x^{m-1}+\ldots+a_m$ ، $a_i\in F$ فإن $q(T)=a_0T^m+a_1T^{m-1}+\ldots+a_m$ ومن ثم فإن

$$vq(T)=v(a_0T^m+a_1T^{m-1}+\ldots+a_m)=a_0(vT^m)+a_1(vT^{m-1})+\ldots+a_mv$$
$$=(a_0\lambda^m+a_1\lambda^{m-1}+\ldots+a_m)v=q(\lambda)v$$

وذلك استنادا إلى الملاحظة الواردة أعلاه. وهكذا فإن $v(q(\lambda)-q(T))=0$. ووفقا لمبرهنة (٦-٢-١) يكون $q(\lambda)$ جذرا مميزا لـ $q(T)$.

وكنتيجة مباشرة لتمهيدية (٦-٢-١) تكون لدينا الحالة الخاصة (والمهمة جدا) الآتية.

مبرهنة (٦-٢-٢)

إذا كان $\lambda\in F$ جذرًا مميزًا لـ $T\in A(V)$ فإن λ يكون جذرًا لكثيرة الحدود الدنيا لـ T. وبصورة خاصة، يوجد عدد منته من الجذور المميزة لـ T في F.

البرهان

لنفرض أن $p(x)$ هي كثيرة الحدود الدنيا لـ T على F ، أي أن $p(T)=0$. إذا كان $\lambda\in F$ جذرًا مميزًا لـ T ، فإنه يوجد متجه $0\neq v\in V$ بحيث يكون $vT=\lambda v$. وكما في برهان تمهيدية (٦-٢-١) $vp(T)=p(\lambda)v$ ، ولكن $p(T)=0$ الأمر الذي يقتضي أن $p(\lambda)v=0$ وحيث إن $v\neq 0$ لذا فإنه يجب أن يكون لدينا $p(\lambda)=0$ مما يعني أن λ جذور لـ $p(x)$. ولما كان عدد جذور $p(x)$ في F منتهيًا (وفي الحقيقة، لما كانت $\deg p(x)\leq n^2$ حيث $n=\dim_F V$ لذا فإن عدد جذور $p(x)$ في F هو على الأكثر n^2) لذلك فإنه يوجد عدد منته فقط من الجذور المميزة لـ T في F.

إذا كان $T\in A(V)$ وكان $S\in A(V)$ منتظما فإن

$(STS^{-1})^2=STS^{-1}STS^{-1}=ST^2S^{-1}$ و $(STS^{-1})^3=ST^3S^{-1},\ldots,(STS^{-1})^i=ST^iS^{-1}$.

وبالتالي فإنه لأي $q(x)\in F[x]$ يكون $q(STS^{-1})^i=Sq(T)S^{-1}$. وخصوصا، إذا كان $q(T)=0$ فإن $q(STS^{-1})=0$. وهكذا إذا كان $q(x)$ هي كثيرة الحدود الدنيا لـ T، فإنه ينتج بسهولة أن $p(x)$ هي كثيرة الحدود الدنيا لـ STS^{-1}. بهذا نكون قد برهنا على التمهيدية الآتية.

تمهيدية (٦-٢-٢)

إذا كان $T,S\in A(V)$ وكان S منتظما فإن T و STS^{-1} لهما نفس كثيرة الحدود الدنيا.

تعريف

*يقال عن المتجه $0\neq v\in V$ إنه **متجه مميز** (characteristic vector) تابع للجذر المميز $\lambda\in F$ إذا كان $vT=\lambda v$.*

ما هي العلاقة، وذلك في حالة وجودها، التي يجب أن تتوفر بين المتجهات المميزة لـ T والتي تتبع الجذور المميزة المختلفة؟ إن الاجابة على ذلك هي في المبرهنة الآتية.

مبرهنة (٦-٢-٣)

إذا كانت $\lambda_1,\ldots,\lambda_k\in F$ هي الجذور المميزة لـ $T\in A(V)$ وكانت $v_1,\ldots,v_k$ هي المتجهات المميزة لـ T التابعة للجذور المميزة $\lambda_1,\ldots,\lambda_k$ على الترتيب فإن $v_1,\ldots,v_k$ مستقلة خطيا على F.

البرهان

عندما $k=1$ لا يوجد شيء يتطلب البرهان. لذلك نفرض أن $k>1$. إذا كانت $v_1,\ldots,v_k$ مرتبطة خطيا على F، فإنه يوجد علاقة على الشكل $\alpha_1v_1+\ldots+\alpha_kv_k=0$، حيث $\alpha_1,\ldots,\alpha_k\in F$ كما أنها ليست كلها أصفارا. في جميع العلاقات التي من هذا النوع، يوجد علاقة تكون فيها المعاملات غير الصفرية أقل ما يمكن، وبترقيم المتجهات بطريقة مناسبة فإنه يمكن أن نفرض أن أقصر علاقة هي:

$$\beta_1v_1+\ldots+\beta_jv_j=0\ ,\ \beta_1\neq0,\ldots,\beta_j\neq0 \qquad (1)$$

الآن نؤثر بـ T على المعادلة (١) مع الأخذ بعين الاعتبار أن $v_iT=\lambda_i v_i$ فنحصل على

$$\lambda_1\beta_1 v_1+\ldots+\lambda_j\beta_j v_j=0 \qquad (٢)$$

بضرب المعادلة (١) بـ λ_1 ثم الطرح من المعادلة (٢) نجد

$$(\lambda_2-\lambda_1)\beta_2 v_2+\ \ldots\ +(\lambda_j-\lambda_1)\beta_j v_j=0$$

الآن إن $\lambda_i-\lambda_1\neq 0$ عندما $i>1$ كما أن $\beta_i\neq 0$ ومن ثم فإن $(\lambda_i-\lambda_1)\beta_i\neq 0$ ولكننا بهذا نكون قد حصلنا على علاقة بين المتجهات $v_1,v_2,\ldots,v_k$ أقصر من التي في (١). وبهذا التناقض يتم إثبات المبرهنة.

نتيجة (١)

إذا كان $T\in A(V)$ وكان $dim_F V=n$ فإن عدد جذور T المميزة المختلفة في F لا يمكن أن يزيد عن n.

البرهان

إن أية مجموعة من المتجهات المستقلة خطيا في V يمكن أن تحتوي على الأكثر على n من العناصر. وحيث إنه يمكن أن ينشأ عن أية مجموعة من الجذور المميزة لـ T مجموعة مقابلة من المتجهات المميزة المستقلة خطيًّا وذلك وفقا لمبرهنة (٦-٢-٣) فإن بهذا يكون قد تم برهان النتيجة.

نتيجة (٢)

إذا كان $T\in A(V)$ وكان $dim_F V=n$ وإذا كان عدد جذور T المميزة المختلفة في F هو n فإنه يوجد أساس لـ V على F يتكون من متجهات T المميزة.

سنترك برهان هذه النتيجة للقارىء. إن نتيجة (٢) تعتبر الأولى من مبرهنات سنتطرق إليها. إنها تنص على أنه يوجد أساس معين لفضاء المتجهات يجعل وصف تحويل خطي معيّن سهلا.

مسائل

في هذه المسائل سيكون V فضاء متجهات منتهي البعد على F .

١ ـ إذا كان $T\in A(V)$ و $q(x)\in F[x]$ بحيث أن $q(T)=0$. فهل صحيح أن كل جذر لـ $q(x)$ هو جذر مميز لـ T ؟ برهن على أن إما هذا صحيح ، أو أورد مثالا تثبت فيه أن هذا غير صحيح .

٢ ـ إذا كان $T\in A(V)$ وكانت $p(x)$ هي كثيرة حدود T الدنيا على F وإذا كانت جميع جذور $p(x)$ تنتمي إلى F. فأثبت أن كل جذر لـ $p(x)$ هو جذر مميز لـ T.

٣ ـ ليكن بعد الفضاء V على F يساوي 2 حيث F هو حقل الأعداد الحقيقية وليكن أساس V هو v_1,v_2. أوجد الجذور المميزة وكذلك المتجهات المميزة المقابلة لـ T المعرف كما يلي :

(ا) $v_1T=v_1+v_2\ ,\ v_2T=v_1-v_2$

(ب) $v_1T=5v_1+6v_2\ ,\ v_2T=-7v_2$

(جـ) $v_1T=v_1+2v_2\ ,\ v_2T=3v_1+6v_2$

٤ ـ إذا كان V هو كما ورد في المسألة (٣) وكان $T\in A(V)$ معرف كما يلي : $v_1T=\alpha v_1+\beta v_2\ ,\ v_2T=\gamma v_1+\delta v_2$ ، حيث $\alpha,\beta,\gamma,\delta\in F$.

(ا) أوجد الشروط اللازمة والكافية لكي يكون الصفر جذرا مميزًا لـ T وذلك بدلالة $\alpha,\beta,\gamma,\delta$.

(ب) أوجد الشروط اللازمة والكافية لكي يكون لـ T جذران مميزان مختلفان وذلك بدلالة $\alpha,\beta,\gamma,\delta$.

٥ ـ إذا كان بعد V على F يساوي 2. فأثبت أن كل عنصر من $A(V)$ يحقق كثيرة حدود درجتها على F تساوي 2.

٦* ـ إذا كان بعد V على F يساوي 2 وكان $S,T\in A(V)$. فأثبت أن $(ST-TS)$ يتبادل مع جميع عناصر $A(V)$.

٧ ـ برهن على نتيجة (٢) التابعة لمبرهنة (٦-٢-٣) .

٨ ـ إذا كان بعد V على F هو n وكان $T\in A(V)$ معدوم القوى، (أي أن $T^k=0$ ، لعدد

ما k) فأثبت أن $T^n=0$ (*إرشـــاد*: إذا كان $v\in V$ فاستخدم كون العناصر $v,vT,vT^2,\ldots,vT^n$ مرتبطة خطيًّا على F.

(٦-٣) المصفــوفــات

على الرغم من أننا ناقشنا التحويلات الخطية منذ بعض الوقت إلا أن مناقشتنا تلك لم تتـطرق إلى تفاصيل دقيقة تتعلق بتلك التحويلات، إذ أن التحويل الخطي بالنسبة لنا كان مجرد رمز (غالبا هو T) يؤثر بطريقة معيّنة على فضاء متجهات. وعندما نركز التفكير في الموضوع خارج نطاق الأمثلة القليلة التي واجهناها في المسائل، فإننا في الحقيقة لم نواجه بعد تحويلاً خطيًّا معيّنًا بحد ذاته، لذا فإنه من الواضح أنه لغرض متـابعة الموضوع إلى أبعد من ذلك فإنه ستكون هناك حاجة لدراسة مفصلة وكاملة لتحويل خطي مفروض. ولنذكر مسألة معيّنة تتعلق بالتحويل (ولنفرض، جدلا، في الوقت الحاضر أن لدينا الوسائل لإدراكها) وهي: كيف نجد الجذور المميزة لتحويل خطي بطريقة عملية؟

إن ما نبحث عنه هي طريقة بسيطة لعرض التحويل الخطي، أو بعبارة أكثر دقة طريقة بسيطة لتمثيله. إننا سوف ننجز هذا باستخدام أساس خاص لفضاء المتجهات وأيضا باستخدام تأثير هذا التحويل الخطي على هذا الأساس. وعندما يتم إنجاز مثل هذا، فإنه باستخدام العمليات في A(V) يمكننا استحداث عمليات للرموز الجديدة بحيث نجعل منها جبراً. إن هذا الشيء الجديد، مفعما بالروح الجبرية، يمكن دراسته كموضوع رياضي شيق في حد ذاته. هذه الدراسة هي التي تشمل موضوع نظرية *المصفوفات*.

ومع ذلك، فإن تجاهل أصل المصفوفات، بمعنى دراسة مجموعة الرموز مستقلة عما تمثل، يمكن أن يكون مكلفا ذلك لأننا نستبعد مقدارًا عظيمًا من المعلومات المفيدة. وبدلا من ذلك، فإننا سنستخدم، دائما، التفاعل بين النظام المجرد، A(V)، والنظام الملموس، الذي هو جبر المصفوفات للحصول على معلومات عن أحدهما من الآخر.

ليكن V فضاء متجهات بعده n على الحقل F وليكن $v_1,\ldots,v_n$ هو أساس V على F. فإذا كان $T\in A(V)$ فإنه يمكن تعيين T على متجه بمجرد معرفتنا لتأثيره على أساس V.

ولما كان T يطبق V إلى نفسه فإن $v_1T,\ldots,v_nT$ يجب أن تكون كلها في V. وكل عنصر من هذه العناصر، باعتبارها عناصر من V ، يمكن كتابتها بطريقة وحيدة كتركيب خطي للعناصر $v_1,\ldots,v_n$ على F.

وهكذا فإن :

$$\begin{aligned}
v_1T&=\alpha_{11}v_1+\alpha_{12}v_2+\ldots+\alpha_{1n}v_n\\
v_2T&=\alpha_{21}v_1+\alpha_{22}v_2+\ldots+\alpha_{2n}v_n\\
v_iT&=\alpha_{i1}v_1+\alpha_{i2}v_2+\ldots+\alpha_{in}v_n\\
&\vdots\\
v_nT&=\alpha_{n1}v_1+\alpha_{n2}v_2+\ldots+\alpha_{nn}v_n
\end{aligned}$$

حيث كل من $a_{ij}\in F$. إنه يمكن كتابة هذا النظام مع المعادلات باختصار على الصيغة :

$$v_iT=\sum_{j=1}^{n}a_{ij}v_j \quad ; \quad i=1,2,\ldots,n$$

إن مجموعة الأعداد المرتبة a_{ij} في F والتي عددها n^2 ، تصف T تماما . كما يمكن استخدامها لتمثيل T.

تعريف

*ليكن V فضاء متجهات بعده على F هو n وليكن $v_1,\ldots,v_n$ هو أساس V على F. إذا كان $T\in A(V)$ فإن **مصفوفة** (Matrix) T بالنسبة للأساس $v_1,\ldots,v_n$ وتكتب بالصورة m(T) هي :*

$$m(T)=\begin{pmatrix}\alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n}\\ \vdots & \vdots & & \vdots\\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn}\end{pmatrix}$$

حيث $v_iT=\sum_j a_{ij}v_j$.

المصفوفة، عندئذ، هي صفيف مربع من عناصر F بدون أي خواص إضافية بعد والتي تمثل تأثير تحويل خطي على أساس معطى.

دعنا نفحص المثال الآتي: ليكن F حقلا و V مجموعة كثيرات الحدود في x من الدرجة n-1 أو أقل على F. ولنعرف على V التحويل D بالقاعدة.

$$(\beta_0+\beta_1 x+\ldots+\beta_{n-1}x^{n-1})D=\beta_1+2\beta_2 x+\ldots+i\beta_i x^{i-1}+\ldots+(n-1)\beta_{n-1}x^{n-2}$$

من الواضح أن D تحويل خطي على V وهو في الحقيقة مؤثر التفاضل.

ما هي مصفوفة D ؟ إن السؤال يبقى بدون معنى ما لم نحدد أساسا لـ V. لنحسب أولا مصفوفة D بالنسبة للأساس

$$v_1=1, v_2=x, v_3=x^2, \ldots, v_i=x^{i-1}, \ldots, v_n=x^{n-1}$$

الآن:

$$v_1D=1D=0=0v_1+0v_2+\ldots+0v_n$$

$$v_2D=xD=1=1v_1+0v_2+\ldots+0v_n$$

$$\vdots$$

$$v_iD=x^{i-1}D=(i-1)x^{i-2}=0v_1+0v_2+\ldots+0v_{i-2}+(i-1)v_{i-1}+0v_i+\ldots+0v_n$$

$$\vdots$$

$$v_nD=x^{n-1}D=(n-1)x^{n-2}=0v_1+0v_2+\ldots+0v_{n-2}+(n-1)v_{n-1}+0v_n$$

بالرجوع إلى تعريف مصفوفة التحويل الخطي بالنسبة لأساس مفروض نرى أن مصفوفة D بالنسبة للأساس $v_1,\ldots,v_n$، أي $m_1(D)$ هي

$$m_1(D)=\begin{pmatrix} 0 & 0 & 0 & \ldots\ldots\ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots\ldots\ldots & 0 & 0 \\ 0 & 2 & 0 & \ldots\ldots\ldots & 0 & 0 \\ 0 & 0 & 3 & \ldots\ldots\ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots\ldots & (n-1) & 0 \end{pmatrix}$$

رغم هذا، فإنه لا يوجد أي خصوصية للأساس المستعمل أو بكيفية ترتيب عناصره.

لنفرض أننا أعدنا ترتيب عناصر هذا الأساس، عندئذ نحصل على أساس آخر هو:

$$w_1=x^{n-1}, w_2=x^{n-2}, \ldots, w_i=x^{i-1}, \ldots, w_n=1$$

ما هي مصفوفة التحويل الخطي D نفسه بالنسبة لهذا الأساس؟

الآن:

$$w_1D=x^{n-1}D=(n-1)\ x^{n-2}=0w_1+(n-1)\ w_2+0w_3+\ldots 0w_n$$

$$\vdots$$

$$w_iD=x^{n-i}D=(n-i)\ x^{n-i-1}=0w_1+\ldots+0w_i+(n-i)w_{i+1}+0w_{i+2}+\ldots+0w_n$$

$$\vdots$$

$$w_nD=1D=0=0w_1+0w_2+\ldots+0w_n$$

ومن ثم فإن $m_2(D)$ ، أية مصفوفة D بالنسبة لهذا الأساس هي:

$$m_2(D)=\begin{pmatrix} 0 & (n-1) & 0 & \ldots & 0 & \ldots & 0 & 0 \\ 0 & 0 & (n-2) & \ldots & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & (n-3) & \ldots & 0 & 0 \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \vdots & & & & & & & \\ 0 & 0 & 0 & \ldots & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 \end{pmatrix}$$

قبل أن نترك هذا المثال، دعنا نحسب مصفوفة D بالنسبة لأساس آخر لـ V على F.

لنفرض أن:

$$u_1=1, u_2=1+x, u_3=1+x^2, \ldots, u_n=1+x^{n-1}$$

من السهل التأكد من أن $u_1, \ldots, u_n$ هو أساس لـ V على F. ما هي مصفوفة D بالنسبة لهذا الأساس؟

لما كان:

$$u_1D=1D=0=0u_1+0u_2+\ldots+0u_n$$

$$u_2D=(1+x)D=1=1u_1+0u_2+\ldots+0u_n$$

$$u_3D=(1+x^2)D=2x=2(u_2-u_1)=-2u_1+2u_2+0u_3+\ \ldots\ +0u_n$$

$$\vdots$$

$$u_nD=(1+x^{n-1})D=(n-1)x^{n-2}=(n-1)(u_n-u_1)$$

$$=-(n-1)u_1+0u_2+\ldots+0u_{n-2}+(n-1)u_{n-1}+0u_n$$

فإن مصفوفة D بالنسبة لهذا الأساس، أي $m_3(D)$ هي

$$m_3(D)=\begin{pmatrix} 0 & 0 & 0 \ldots\ldots & 0 & 0 \\ 1 & 0 & 0 \ldots\ldots & 0 & 0 \\ -2 & 2 & 0 \ldots\ldots & 0 & 0 \\ -3 & 0 & 3 \ldots\ldots & 0 & 0 \\ \vdots & \vdots & \vdots \ \ldots\ldots & \vdots & \vdots \\ -(n-1) & 0 & 0 \ldots & (n-1) & 0 \end{pmatrix}$$

من هذا المثال نرى أن مصفوفات D، بالنسبة للأساسات الثلاثة المستخدمة تعتمد تماما على الأساس. وعلى الرغم من اختلاف هذه الأساسات، فإن المصفوفات المختلفة تمثل نفس التحويل الخطي D كما أننا نستطيع تكوين D من أية واحدة منها متى ما عرفنا الأساس المستخدم في تعيينها. وعلى الرغم من اختلاف هذه المصفوفات فإننا نتوقع وجود علاقة ما بين المصفوفات $m_1(D)$ و $m_2(D)$ و $m_3(D)$ وسنعين هذه العلاقة تماما فيما بعد.

و لما كان الأساس المستخدم في كل مرة هو في متناول أيدينا، فإنه إذا كان لدينا تحويل خطي T (والذي تعريفه، بالطبع لا يعتمد على أساس لفضاء المتجهات) فإن من الطبيعي، بالنسبة لنا، أن نبحث عن أساس يجعل مصفوفة T تأخذ شكلا جميلا. فعلى سبيل المثال، إذا كان T تحويلاً خطيًّا على V الذي بعده على F هو n وإذا كانت جذور T المميزة المختلفة في F هي $\lambda_1,\ldots,\lambda_n$ فإنه من نتيجة ٢ التابعة لمبرهنة (٦-٢-٣) نستطيع إيجاد أساس $v_1,\ldots,v_n$ لـ V على F بحيث يكون $v_iT=\lambda_i v_i$. وبالتالي فإنه بالنسبة لهذا الأساس ستأخذ مصفوفة T شكلا أبسط هو:

$$m(T)=\begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

لقد رأينا، أنه متى ما تم اختيار أساس لـ V فإنه يمكن أن نربط مصفوفة لكل تحويل خطي، والعكس صحيح، أي إذا اخترنا الأساس $v_1,\ldots,v_n$ لـ V على F وإذا كانت لدينا المصفوفة

$$\begin{pmatrix} \alpha_{11} & \ldots\ldots & \alpha_{1n} \\ \vdots & & \\ \alpha_{n1} & \ldots\ldots & \alpha_{nn} \end{pmatrix}, \ a_{ij}\in F$$

فإنه ينشأ عنها تحويل خطي T معرف على V بالقاعدة: $v_iT=\sum_j a_{ij}v_j$. لاحظ أن مصفوفة التحويل الخطي المكوّنة آنفا بالنسبة للأساس $v_1,\ldots,v_n$ هي تماما تلك المصفوفة التي بدأنا بها. وهكذا نجد أن أي صفيف مربع يمكن أن يقوم مقام مصفوفة تحويل خطي ما بالنسبة للأساس $v_1,\ldots,v_n$.

إن العبارات الآتية: الصف الأول، الصف الثاني، . . . الخ للمصفوفة، وكذلك العبارات: العمود الأول، والعمود الثاني، . . . الخ في المصفوفة واضحة.

$$\begin{pmatrix} \alpha_{11} \cdots\cdots \alpha_{1n} \\ \vdots \\ \alpha_{n1} \cdots\cdots \alpha_{nn} \end{pmatrix}$$

سنشير إلى العنصر α_{ij} في الصف رقم i والعمود رقم j بأنه ذلك العنصر في الموضع (i,j) من المصفوفة.

إن كتابة المصفوفة بالشكل الوارد سابقا ليس مريحًا، ولذلك سنكتب المصفوفة دائما على الصيغة (α_{ij}) على أن العنصر في الموضع (i,j) من المصفوفة هو α_{ij}.

لنفرض أن V فضاء متجهات بعده على F هو n وأن $v_1,\ldots,v_n$ هو أساس V على F والذي سيبقى بدون تغيير في المناقشة التالية. لنفرض أن T و S هما تحويلان خطيان لـ V على F مصفوفتاهما $m(T)=(\tau_{ij})$ و $m(S)=(\sigma_{ij})$ على الترتيب بالنسبة للأساس المعطى. إن هدفنا هو تحويل البنية الجبرية لـ A(V) إلى مجموعة المصفوفات التي عناصرها في F.

أولا وقبل كل شيء، يكون S=T إذا وفقط إذا كان vS=vT لأي $v\in V$ ومن ثم فإن S=T إذا وفقط إذا كان $v_iS=v_iT$ لأي متجهات $v_1,\ldots,v_n$ تكون أساسا لـ V على F. بعبارة أخرى S=T إذا وفقط إذا كان $\sigma_{ij}=\tau_{ij}$ لكل i ولكل j.

إذا كان $m(S)=(\sigma_{ij})$ و $m(T)=(\tau_{ij})$ فهل من الممكن تعيين m(S+T)؟ بما أن $m(S)=(\sigma_{ij})$ فإن $v_iS=\sum_j\sigma_{ij}v_j$ وبالمثل $v_iT=\sum_j\tau_{ij}v_j$ وبناء عليه فإن

$$v_i(S+T)=v_iS+v_iT=\sum_j\sigma_{ij}v_j+\sum_j\tau_{ij}v_j=\sum_j(\sigma_{ij}+\tau_{ij})v_j$$

ولكن استنادا إلى تعريف مصفوفة التحويل الخطي بالنسبة لأساس معطى يكون $m(S+T)=(\lambda_{ij})$، حيث $\lambda_{ij}=\alpha_{ij}+\tau_{ij}$ لكل i ولكل j. وبطريقة مماثلة نثبت أنه إذا كان $\gamma\in F$ فإن $m(\gamma S)=(\mu_{ij})$، حيث $\mu_{ij}=\gamma\sigma_{ij}$، لكل i ولكل j.

إن الحساب الأكثر تعقيداً هو حساب $m(ST)$.

الآن

$$v_i(ST)=(v_iS)T=(\sum_k \sigma_{ik}v_k)T=\sum_k \sigma_{ik}(v_kT)$$

ولكن :

$$v_kT=\sum_j \tau_{kj}v_j$$

بالتعويض في الصيغة الواردة أعلاه نحصل على :

$$v_i(ST)=\sum_k \sigma_{ik}(\sum_j \tau_{kj}v_j)=\sum_j(\sum_k \sigma_{ik}\tau_{kj})v_j$$

(أثبت ذلك) . ولذلك فإن $m(ST)=\lambda_{ij}$ حيث $v_{ij}=\sum_k \sigma_{ik}\tau_{kj}$ لكل i ولكل j.

من أول نظرة يبدو أن حساب مصفوفة حاصل ضرب تحويلين خطيين بالنسبة لأساس ما معقد. ومع ذلك، نلاحظ أن العنصر في الموضع (i,j) في m(ST) يمكن الحصول عليه كما يلي. اعتبر صفوف S على أنها متجهات وكذلك أعمدة T. عندئذ يكون العنصر في الموضع (i,j) من المصفوفة m(ST) هو حاصل الضرب الداخلي للصف رقم i في S بالعمود رقم j في T.

ولنوضح هذا بالمثال الآتي. لنفرض أن

$$m(T)=\begin{pmatrix}-1 & 0\\ 2 & 3\end{pmatrix} \quad \text{وأن} \quad m(S)=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$$

عندئذ يكون حاصل الضرب الداخلي للصف الأول من S بالعمود الأول من T هو $3=(2)(2)+(1)(-1)$ لذلك فإن العنصر في الموضع (1,1) من المصفوفة m(ST) هو 3.
كما أن حاصل الضرب الداخلي للصف الأول من S بالعمود الثاني من T هو $6=(3)(2)+(0)(1)$ وبالتالي فإن العنصر في الموضع (1,2) من المصفوفة m(ST) هو 6.
أيضا إن حاصل الضرب الداخلي للصف الثاني من S بالعمود الأول من T هو $5=(2)(4)+(-1)(3)$ وعليه فإن العنصر في الموضع (2,1) من المصفوفة m(ST) هو 5.
وأخيرا فإن حاصل الضرب الداخلي للصف الثاني من S بالعمود الثاني من T هو $12=(3)(4)+(0)(3)$ وعليه فإن العنصر في الموضع (2,2) من المصفوفة m(ST) هو 12.

وهكذا فإن :

$$m(ST)=\begin{pmatrix} 3 & 6 \\ 5 & 12 \end{pmatrix}$$

إن الهدف من المناقشة السابقة هو تهيئة الطريق للإنشاءات التي نحن على وشك البدء بها .

ليكن F حقلا . إن *المصفوفة* من النوع n×n على F هي **الصفيف** (array) المربع من العناصر في F ، أي

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \ldots & \alpha_{1n} \\ \vdots & \vdots & \vdots \\ \alpha_{n1} & \alpha_{n2} \ldots & \alpha_{nn} \end{pmatrix}$$

(والتي سنكتبها على الشكل (α_{ij})). لتكن :

$$F_n=\{(\alpha_{ij})|\alpha_{ij}\in F\}$$

سنقدم في F_n فكرة التساوي بين عناصرها، الجمع، والضرب بعناصر من F وكذلك الضرب بحيث نجعل منها جبراً على F ، كما سنستخدم خواص m(T) حيث $T\in A(V)$ وذلك كمرشد لنا .

١) نعـــرف $(\alpha_{ij})=(\beta_{ij})$ وذلـــك لأية مصفـــوفتـين من F_n إذا وفقط إذا كان $\alpha_{ij}=\beta_{ij}$ لكل i و j.

٢) نعرف $(\alpha_{ij})+(\beta_{ij})=(\lambda_{ij})$ ، حيث $\lambda_{ij}=\alpha_{ij}+\beta_{ij}$ لكل i و j.

٣) نعرف، من أجل $\gamma\in F$ ، $\gamma(\alpha_{ij})=(\mu_{ij})$ ، حيث $\mu_{ij}=\gamma\alpha_{ij}$ لكل i و j.

٤) نعرف $(\alpha_{ij})(\beta_{ij})=(v_{ij})$ حيث $v_{ij}=\sum_k \alpha_{ik}\beta_{kj}$ لكل i و j.

ليكن V فضاء متجهات بعده n على F وليكن $v_1,\ldots,v_n$ هو أساس V على F. إن المصفـوفـة m(T) بالنسبة للأساس $v_1,\ldots,v_n$ تربط $T\in A(V)$ بعنصر m(T) في F_n. إننا ندعي أن التطبيق من A(V) إلى F_n الذي يطبق T على m(T) هو تماثل جبري من A(V) على F_n. ووفقا لهذا التماثل يكون F_n جبراً تجميعيًا على F (ويمكن التحقق من ذلك مباشرة) . نطلق على F_n *جبر جميع المصفوفات من النوع n×n على F.*

إن كل أسـاس لـ V يزودنا بتماثل جبري من $A(V)$ على F_n. هذا ومن الممكن البرهان على أن كل تماثل جبري من $A(V)$ على F_n يمكن الحصول عليه بهذه الطريقة.

وعلى ضوء الطبيعية الخاصة لكل تماثل بين $A(V)$ و F_n، فإننا سنطابق أحيانا التحويل الخطي بمصفوفته وذلك بالنسبة لأساس ما، كما سنطابق بين $A(V)$ و F_n. في الحقيقة، يمكن اعتبار F_n على أنه $A(V)$ الذي يؤثر على فضاء المتجهات $V=F^{(n)}$ المكون من جميع النونيات المرتبة على F، حيث تؤثر $(\alpha_{ij})\in F_n$ على الأساس المكون من

$$v_1=(1,0,..,0),\ v_2=(0,1,0,\ldots,0),\ \ldots,\ v_n=(0,0,\ldots,0,1)$$

بالقاعدة: $v_i(\alpha_{ij})$ = الصف رقم i في (α_{ij}).

نلخص ما ورد سابقا بالمبرهنة التالية:

مبرهنة (٦-٣-١)

إن مجموعة جميع المصفوفات من النوع $n\times n$ تشكل جبرا على F يرمز له بالرمز F_n. وإذا كان V فضاء متجهات على F بعده n فإن $A(V)$ و F_n متماثلان باعتبار كل منهما جبر على F. وإذا كان $v_1,\ldots,v_n$ أساسًا لـ V على F وكانت $m(T)$ هي مصفوفة $T\in A(V)$ بالنسبة للأساس $v_1,\ldots,v_n$ فإن التطبيق $T\rightarrow m(T)$ هو تماثل جبري من $A(V)$ على F_n.

إن العنصر الصفري في F_n بالنسبة لعملية الجمع هو المصفوفة الصفرية وهي التي جميع عناصرها أصفار وغالبا ما سنكتبها على الشكل 0. إن مصفوفة الوحدة، التي هي عنصر الوحدة في F_n بالنسبة للضرب هي المصفوفة التي عناصرها القطرية 1 وأصفار في سوى ذلك وسنكتبها على الشكل I أو I_n (وذلك عندما نريد التأكيد على سعتها) أو حتى على الشكل 1. وإذا كان $\alpha\in F$ فإن المصفوفة

$$\alpha I=\begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix}$$

(الفـراغـات الخـالية تدل على أنها عنـاصر صفـرية) **تدعى بالمصفـوفـة القيـاسيـة**

(scalar matrix) بالنـظر إلى التماثل بين $A(V)$ و F_n فإن من الواضح أن لـ $T\in A(V)$ معكوس إذا وفقط إذا كان للمصفوفة $m(T)$ معكوس في F_n.

إذا كان لدينا تحويل خطي واخترنا الأساسين $v_1,\ldots,v_n$ و $w_1,\ldots,w_n$ لـ V على F فإنه ينشأ عن كل أساس مصفوفة هما $m_1(T)$ و $m_2(T)$ وهما مصفوفتا T بالنسبة للأساسين المذكورين على الترتيب. ما هي العلاقة بين $m_1(T)$ و $m_2(T)$ وذلك باعتبارهما مصفوفتين أو باعتبارهما عنصرين من جبر المصفوفات F_n ؟

مبرهنة (٦-٣-٢)

إذا كان V فضاء متجهات بعده على F هو n وكانت مصفوفة $T\in A(V)$ بالنسبة للأساس $v_1,\ldots,v_n$ لـ V على F هي $m_1(T)$ ومصفوفته بالنسبة للأساس $w_1,\ldots,w_n$ لـ V على F هي $m_2(T)$ فإنـه يوجـد عنصر $C\in F_n$ بحيث يكون $m_2(T)=Cm_1(T)C^{-1}$. وفي الحقيقة إذا كان S تحويلاً خطيًا على V معرفًا بالقاعدة $v_iS=w_i$ ، $i=1,2,\ldots,n$ فإنه يمكن اختيار C لتكون $m_1(S)$.

البرهان

لنفـــرض أن $m_1(T)=(\alpha_{ij})$ و $m_2(T)=(\beta_{ij})$ ، عندئـــذ $v_iT=\sum\alpha_{ij}v_j$ $w_iT=\sum\beta_{ij}w_j$. لنفرض أن S هو التحويل الخطي على V المعرف بالقاعدة $v_iS=w_i$. لما كان $v_1,\ldots,v_n$ ، $w_1,\ldots,w_n$ أساسين لـ V على F ولما كان S يطبق V على نفسه، فإنه وفقا لمبرهنة (٦-١-٤) يوجد معكوس لـ S في $A(V)$.

الآن $w_iT=\sum_j\beta_{ij}w_j$ وحيث إن $w_i=v_iS$ ، فإنه بالتعويض عن w_iT نحصـل على $(v_iS)T=\sum_j\beta_{ij}(v_jS)$. ولكن، عندئذ

$$v_i(ST)=\sum_j(\beta_{ij}v_j)S$$

وحيث إنه يوجد معكوس لـ S فإنه يمكن تبسيط هذا إلى $v_i(STS^{-1})=\sum_j\beta_{ij}v_j$. واستنادا إلى تعريف مصفوفة التحويل الخطي بالنسبة لأساس مفروض يكون

$$m_1(STS^{-1})=(\beta_{ij})=m_2(T)$$

ومع ذلك، فإن التطبيق $T\to m_1(T)$ هو تماثل من $A(V)$ على F_n. ولذلك فإن

$$m_1(STS^{-1})= m_1(S)m_1(T)m_1(S^{-1})=m_1(S)m_1(T)m_1(S)^{-1}$$

وبضم هذه المعلومات مع بعضها نحصل على

$$m_2(T)=m_1(S)m_1(T)m_1(S)^{-1}$$

وهذا هو تماما ما تدعيه المبرهنة.

نوضح المبرهنة الأخيرة بمثال وهو مصفوفة التحويل D الذي سبق وإن درسناه وذلك بالنسبة للأسس المختلفة. لاختصار الحسابات سنفرض أن V هو فضاء كثيرات الحدود على F من الدرجة الثالثة أو أقل. وأن D هو مؤثر التفاضل المعرف بالقاعدة

$$(\alpha_0+\alpha_1x+\alpha_2x^2+\alpha_3x^3)D=\alpha_1+2\alpha_2x+3\alpha_3x^2$$

وكما رأينا، سابقا، فإن مصفوفة D بالنسبة للأساس $v_1=1,v_2=x,v_3=x^2,v_4=x^3$ هي:

$$m_1(D)=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

كما أن مصفوفة D بالنسبة للأساس $u_1=1,\ u_2=1+x,\ u_3=1+x^2,\ u_4=1+x^3$ هي:

$$m_2(D)=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 \\ -3 & 0 & 3 & 0 \end{pmatrix}$$

ليكن S هو التحويل الخطي المعرف بالقاعدة:

$$v_1S=w_1(=v_1),\ v_2S=w_2=1+x=v_1+v_2$$

$$v_3S=w_3=1+x^2=v_1+v_3,\ v_4S=w_4=1+x^3=v_1+v_4$$

عندئذ تكون مصفوفة S بالنسبة للأساس v_1,v_2,v_3,v_4 هي:

$$C=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

وبحساب بسيط يتضح لنا أن

$$C^{-1}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

وعندئذ:

$$Cm_1(D)C^{-1}=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

$$=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 \\ -3 & 0 & 3 & 0 \end{pmatrix}=m_2(D)$$

وذلك كما يجب أن يكون، وفقا للمبرهنة (تحقق من جميع الحسابات المستخدمة!).

إن المبرهنة تؤكد على أن معرفة مصفوفة التحويل الخطي بالنسبة لأي أساس تسمح لنا بحسابها لأي أساس آخر ما دمنا نعرف التحويل الخطي (أو المصفوفة) الذي يغير الأساس.

إننا لم نجب بعد على السؤال: إذا كان لدينا تحويل خطي فكيف يمكن حساب جذوره المميزة؟ إن هذا سيأتي فيما بعد. وسنرى أنه بمعرفة مصفوفة التحويل الخطي كيف يمكن تكوين كثيرة حدود جذورها هي بالضبط الجذور المميزة للتحويل الخطي.

مسائل

١ - احسب حاصل ضرب المصفوفات الآتية:

ا) $$\begin{pmatrix} 1 & 2 & 3 \\ 1 & -1 & 3 \\ 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 3 \\ -1 & -1 & -1 \end{pmatrix}$$

ب) $\begin{pmatrix} 1 & 6 \\ -6 & 1 \end{pmatrix}\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}$

جـ) $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}^2$

د) $\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}^2$

٢ ـ تحقق من جميع الحسابات الواردة في المثال الموضح لمبرهنة (٦ـ٣ـ٢) .

٣ ـ برهن باستخدام تعريف الجمع والضرب في F_n أن

ا) $A(B+C)=AB+AC$

ب) $(AB)C=A(BC)$

حيث $A,B,C\in F_n$

٤ ـ أثبت أنه لأي عنصرين $A,B\in F_2$ تكون $(AB-BA)^2$ مصفوفة قياسية .

٥) ليكن V هو فضاء كثيرات الحدود من الدرجة الثالثة أو أقل على F ولنعرف T كما يلي :

$$(\alpha_0+\alpha_1 x+\alpha_2x^2+\alpha_3x^3)T=\alpha_0+\alpha_1 (x+1)+\alpha_2(x+1)^2+\alpha_3(x+1)^3$$

احسب مصفوفة T بالنسبة لكل من الأساسين :

ا) $1,x,x^2,x^3$

ب) $1,1+x,1+x^2,1+x^3$

جـ) إذا كانت المصفوفة في الفقرة (ا) هي A وفي الفقرة (ب) هي B فأوجد مصفوفة C بحيث يكون $B=CAC^{-1}$.

٦ ـ إذا كان $V=F^3$ وكانت :

$$\begin{pmatrix} 1 & 1 & 2 \\ -1 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix}$$

هي مصفوفة $T \in A(V)$ بالنسبة للأساس

$$v_1=(1,0,0),\ v_2=(0,1,0),\ v_3=(0,0,1)$$

فأوجد مصفوفة T بالنسبة لكل من الأساسين

(أ) $u_1=(1,1,1) \quad , \quad u_2=(0,1,1) \quad , \quad u_3=(0,0,1)$

(ب) $u_1=(1,1,0) \quad , \quad u_2=(1,2,0) \quad , \quad u_3=(1,2,1)$

٧ - برهن على أنه إذا كانت

$$A=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & -11 & 6 \end{pmatrix} \in F_3$$

(حيث مميز $F \neq 2$) فإن

(أ) $A^3-6A^2+11A-6=0$

(ب) يوجد مصفوفة $C \in F_3$ بحيث يكون

$$CAC^{-1}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

٨ - أثبت أنه من غير الممكن إيجاد مصفوفة $C \in F_2$ بحيث يكون

$$C \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} C^{-1}=\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

وذلك لأي $\alpha,\beta \in F$.

٩ - يقال إن المصفوفة $A \in F_n$ هي مصفوفة قطرية (Diagonal) إذا كانت جميع عناصرها الواقعة خارج القطر الرئيس أصفارًا، أي أنه إذا كانت $A=(\alpha_{ij})$ فإن $\alpha_{ij}=0$ عندما $i \neq j$. فإذا كانت A مصفوفة قطرية وكانت العناصر في القطر الرئيس مختلفة. فأوجد جميع المصفوفات $B \in F_n$ التي تتبادل مع A ، أي جميع المصفوفات B بحيث يكون $AB=BA$.

١٠ ـ باستخدام نتيجة المسألة (٩). برهن على أن المصفوفات التي تتبادل مع جميع المصفوفات في F_n هي فقط المصفوفات القياسية.

١١ ـ لتكن $A \in F_n$، حيث

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

حيث جميع عناصر A أصفار عدا القطر فوق الرئيس الذي عناصره هي 1. أثبت أن $A^n=0$ ولكن $A^{n-1}\neq 0$

١٢* ـ إذا كانت A كما في مسألة (١١). فأوجد جميع المصفوفات في F_n التي تتبادل مع A ثم أثبت أن هذه المصفوفات يجب أن تأخذ الصيغة

$\alpha_0+\alpha_1A+\alpha_2A^2+\ldots+\alpha_{n-1}A^{n-1}$ ، حيث $\alpha_0,\ldots,\alpha_{n-1}\in F$

١٣ ـ لتكن $A\in F_2$ و $C(A)=\{B\in F_2|AB=BA\}$. ولتكن:

$C(C(A))=\{G\in F_2|GX=XG\ ,$ لكل X في $C(A)\}$

أثبت أنه إذا كانت $G\in C(C(A))$ فإن G تأخذ الصيغة $\alpha_0+\alpha_1A$ حيث $\alpha_0,\alpha_1\in F$.

١٤ ـ حل المسألة (١٣) وذلك في حالة كون $A\in F_3$، مثبتا أنه إذا كانت $G\in C(C(A))$ فإن G تأخذ الصيغة $\alpha_0+\alpha_1A+\alpha_2A^2$.

١٥ ـ لنعرف المصفوفات E_{ij} في F_n كما يلي: E_{ij} هي المصفوفات التي عنصرها الوحيد غير الصفري في الموضع (i,j) هو 1. أثبت أن:

(ا) E_{ij} تشكل أساسًا لـ F_n على F.

(ب) $E_{ij}E_{kl}=0$ ، $j\neq k$ و $E_{ij}E_{jl}=E_{il}$

(جـ) يوجد مصفوفة C بحيث يكون $CE_{ii}C^{-1}=E_{jj}$ ، حيث i ، j عددان مفروضان.

(د) إذا كان $i\neq j$ فإنه يوجد مصفوفة C بحيث يكون $CE_{ij}C^{-1}=E_{12}$

(هـ) أوجد جميع المصفوفات $B\in F_n$ التي تتبادل مع E_{12}.

(و) أوجد جميع المصفوفات $B \in F_n$ التي تتبادل مع E_{11}.

١٦ - ليكن F هو حقل الأعداد الحقيقية و C هو حقل الأعداد المركبة ولنفرض أن $\alpha \in C$ وأن $T_\alpha : C \to C$ معرف بالقاعدة $xT_\alpha = x\alpha$ لكل $x \in C$. باستخدام الأساس 1,i. أوجد مصفوفة التحويل الخطي T_α ثم أوجد صورة مماثلة للأعداد المركبة على هيئة مصفوفات من النوع 2×2 على حقل الأعداد الحقيقية.

١٧ - لتكن Q هي حلقة قسمة الرباعيات على حقل الأعداد الحقيقية. باستخدام الأساس 1,i,j,k لـ Q على F. أوجد (كما في المسألة (١٦)) صورة مماثلة لـ Q على هيئة مصفوفات من النوع 4×4 على حقل الأعداد الحقيقية.

١٨*- استخدم نتيجتي المسألتين (١٦)، (١٧) لإيجاد صورة مماثلة لـ Q على هيئة مصفوفات من النوع 2×2 على حقل الأعداد المركبة.

١٩ - لتكن M هي مجموعة المصفوفات من النوع n×n والتي عناصرها 0 أو 1 بحيث يوجد 1 فقط في كل صف وكل عمود (مثل هذه المصفوفات تدعى **المصفوفات التبديلية** permutation matrix)

(ا) إذا كانت $M \in M$ فصف AM بدلالة صفوف وأعمدة A.

(ب) إذا كانت $M \in M$ فصف MA بدلالة صفوف وأعمدة A.

٢٠ - لتكن M كما في المسألة (١٩). أثبت أن:

(ا) M تحتوي على عناصر عددها !n

(ب) إذا كانت $M \in M$ فإنه يوجد لـ M معكوس في M.

(جـ) أوجد صيغة صريحة للمعكوس في M.

(د) M زمرة مع عملية ضرب المصفوفات.

(هـ) M تماثل، باعتبارها زمرة، S_n ، زمرة التناظر من الدرجة n.

٢١ - لتكن $A = (\alpha_{ij})$ بحيث أنـه لكل i يكون $\sum_j \alpha_{ij} = 1$. أثبت أن 1 جذر مميز لـ A (أي أن 1-A لا يوجد لها معكوس).

٢٢ - لتكن $A = (\alpha_{ij})$ بحيث أنه لكل j يكون $\sum_i a_{ij} = 1$. أثبت أن 1 جذر مميز لـ A.

٢٣ - أوجد الشروط اللازمة والكافية على $\alpha, \beta, \gamma, \delta$ لكي يكون للمصفوفة $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \beta \end{pmatrix}$ معكوس وعندما يوجد لها معكوس فاكتب A^{-1} صريحة.

٢٤ ـ إذا كانت $E \in F_n$ بحيث أن $E^2=E\neq 0$. فأثبت أنه يوجد مصفوفة $C \in F_n$ بحيث يكون:

$$CEC^{-1}=\left(\begin{array}{cccc|c} 1 & 0 & \dots & 0 & 0 \dots 0 \\ 0 & 1 & \dots & 0 & \dots \\ . & . & \dots & . & \dots . \\ . & . & \dots & . & \dots . \\ . & . & \dots & . & \dots . \\ 0 & 0 & \dots & 1 & 0 \dots 0 \\ \hline 0 & & \dots & 0 & 0 \dots 0 \\ 0 & & \dots & 0 & 0 \dots 0 \end{array}\right)$$

بحيث أن المصفوفة في الزاوية العليا اليسرى هي مصفوفة الوحدة من النوع $r\times r$ ، حيث r هي رتبة E.

٢٥ ـ إذا كان F هو حقل الأعداد الحقيقية. فأثبت أنه من غير الممكن إيجاد مصفوفتين $A,B \in F_n$ بحيث يكون $AB-BA=1$

٢٦ ـ إذا كان مميز $F=2$. فأثبت أنه من غير الممكن في F_2 إيجاد مصفوفتين $A,B \in F_2$ بحيث يكون $AB-BA=1$.

٢٧ ـ يقال إن المصفوفة A هي مصفوفة مثلثة إذا كانت جميع عناصرها فوق القطر الرئيس أصفارًا (كما تكون، أيضا، مثلثة فيما لو كانت جميع عناصرها تحت القطر الرئيس أصفارًا).

(ا) إذا كانت A مثلثة وكانت جميع العناصر في القطر الرئيس لا تساوي أصفارًا فأثبت أنه يوجد لـ A معكوس.

(ب) إذا كانت A مثلثة وكان أحد العناصر في القطر الرئيس صفرًا فأثبت أن A شاذة.

٢٨ ـ إذا كانت A مثلثة. فأثبت أن جذورها المميزة هي بالضبط تلك العناصر الواقعة في القطر الرئيس.

٢٩ ـ إذا كانت $N^k=0$ حيث $N \in F_n$. فأثبت أنه يوجد معكوس لـ $1+N$ ثم أوجده على هيئة كثيرة حدود في N.

٣٠ ـ إذا كانت $A \in F_n$ مثلثة وكانت جميع العناصر في القطر الرئيس أصفارًا. فأثبت أن $A^n=0$

٣١ - إذا كانت $A \in F_n$ مثلثة وكانت جميع العناصر في القطر الرئيس تساوي α حيث $0 \neq \alpha \in F$ فأوجد A^{-1}.

٣٢ - ليكن T و S تحويلين خطيين على V بحيث أن مصفوفة S بالنسبة لأساس ما تساوي مصفوفة T بالنسبة لأساس آخر. أثبت أنه يوجد تحويل خطي A على V بحيث يكون $T = ASA^{-1}$.

(٦-٤) الصيغ القانونية: الصيغة المثلثة

ليكن V فضاء متجهات بعده n على الحقل F.

تعريف

يقال إن التحويلين الخطيين $S, T \in A(V)$ ***متشابهان*** *إذا وجد عنصر $C \in A(V)$ له معكوس بحيث يكون $T = CSC^{-1}$.*

يمكن ترجمة هذا التعريف إلى المصفوفات وذلك بالنظر إلى نتائج البند (٦-٣). وفي الحقيقة، لما كان F_n يؤثر تماما مثل $A(V)$ على $F^{(n)}$ فإن التعريف الوارد آنفا يعرف تشابه المصفوفات وعليه فإن $A, B \in F_n$ متشابهتان إذا وجد مصفوفة $C \in F_n$ لها معكوس بحيث يكون $B = CAC^{-1}$.

إن علاقة التشابه المعرفة آنفا على $A(V)$ هي علاقة تكافؤ، كما يدعى فصل التكافؤ **بفصل التشابه**. إذا كان لدينا تحويلان خطيان فكيف نقرر ما إذا كانا متشابهين؟ بالطبع، علينا أن نفحص فصل التشابه لأحدهما لنرى ما إذا كان الآخر ينتمي إليه. ولكن هذا الاجراء ليس عمليا وبدلا من ذلك نحاول إيجاد علامة معيّنة لكل فصل تشابه وطريقة للانتقال من أي عنصر في هذا الفصل إلى هذه العلامة. كما سنثبت وجود تحويلات خطية في كل فصل تشابه التي تأخذ مصفوفاتها شكلاً مقبولاً وذلك بالنسبة لأساس معيّن. سيطلق على مثل هذه المصفوفات **الصيغ القانونية**. وعلى

هذا لكي نقرر ما إذا كان تحويلان خطيان متشابهين يجب علينا أن نحسب الصيغة القانونية لكل منهما ونتأكد من أنهما متساويتان.

إنه يوجد عدد من الصيغ القانونية الممكنة وسندرس ثلاثًا منها وذلك في هذا البند والبنود الثلاثة اللاحقة هذه الصيغ هي الصيغ المثلثية، صيغة جوردان والصيغة القانونية النسبية.

تعريف

يقال إن الفضاء الجزئي W من V غير متغير تحت تأثير $T\in A(V)$ إذا كان $WT\subset W$.

تمهيدية (٦-٤-١)

إذا كان $W\subset V$ غير متغير تحت تأثير T فإن T يُحدث تحويلا خطيا $\bar{T}$ على V/W معرفا بالقاعدة

$$(v+W)\bar{T}=vT+W$$

وإذا كان T يحقق كثيرة الحدود $q(x)\in F[x]$ فإن $\bar{T}$ كذلك. وإذا كانت $p_1(x)$ هي كثيرة الحدود الدنيا لـ $\bar{T}$ على F وكانت $p(x)$ هي كثيرة الحدود الدنيا لـ T فإن $p_1(x)|p(x)$.

البرهان

ليكن $\bar{V}=V/W$. إن عناصر $\bar{V}$، بالطبع، هي المجموعات المشاركة $v+W$ لـ W في V. لنفرض أن $\bar{v}=v+W\in\bar{V}$. ولنعرف $\bar{v}\bar{T}=vT+W$. إن التحقق من أن $\bar{T}$ تحويل خطي على $\bar{V}$ هو أمر بسيط متى ما أثبتنا أن $\bar{T}$ حسن التعريف على $\bar{V}$. لهذا سنحصر اهتمامنا لبرهان هذا الأمر.

لنفرض أن $\bar{v}=v_1+W=v_2+W$ وأن $v_1,v_2\in V$. ويجب أن نثبت أن $v_1T+W=v_2T+W$. لما كان $v_1+W=v_2+W$ لذا فإن $v_1-v_2\in W$ وحيث إن W غير متغير

تحت تأثير T ، لذلك نجد أن $(v_1-v_2)T \in W$ ومن ثم فإن $v_1T-v_2T \in W$ الأمر الذي ينتج عنه أن $v_1T+W=v_2T+W$ كما هو مطلوب . ومن هنا نعلم أن $\bar{T}$ يعرف تحويلا خطيا على $\bar{V}=V/W$.. إذا كان $\bar{v}=v+W \in \bar{V}$. فإن

$$..\bar{v}(\bar{T^2})=vT^2+W=(vT)T+W=(vT+W)\,\bar{T}=((v+W)\bar{T})\bar{T}=\bar{v}(\bar{T})^2$$

أي أن $(\bar{T^2})=(\bar{T})^2$. وبالمثل نجد أن $(\bar{T^k})=(\bar{T})^k$ لأي $k \geq 0$. وبالتالي فإنه لأي كثيرة حدود $q(x) \in F[x]$ يكون $\overline{q(T)}=q(\bar{T})$ ولما كان $\bar{O}$ هو التحويل الصفري على $\bar{V}$ لذا فإنه لأي كثيرة حدود $q(x) \in F[x]$ مع كون $q(T)=0$ نجد أن $0=q(T)=q(\bar{T})$.

لنفرض الآن أن $p_1(x)$ هي كثيرة الحدود الدنيا على F الذي يحققه $\bar{T}$. إذا كان $q(\bar{T})=0$ حيث $q(x) \in F[x]$ فإن $p_1(x)|q(x)$. فإذا كانت $p(x)$ هي كثيرة الحدود الدنيا لـ T على F فإن $p(T)=0$ ومن ثم فإن $p(\bar{T})=0$ وبالتالي فإن $p_1(x)|p(x)$.

لقد رأينا في مبرهنة (٦-٢-٢) أن جميع الجذور المميزة لـ T التي تقع في F هي جذور لكثيرة الحدود الدنيا لـ T على F . *نقول: إن جميع الجذور المميزة لـ T تقع في F إذا كانت جميع جذور كثيرة الحدود الدنيا لـ T على F تقع في F .*

لقد عرفنا في مسألة (٢٧) في نهاية البند السابق المصفوفة *المثلثة* بأنها تلك المصفوفة التي جميع عناصرها التي فوق القطر الرئيس أصفارًا . وبعبارة أخرى، إذا كان T تحويلاً خطيًا لـ V على F فإن مصفوفة T بالنسبة للأساس $v_1,\ldots,v_n$ تكون مثلثة إذا كان

$$v_1T=\alpha_{11}v_1$$
$$v_2T=\alpha_{21}v_1+\alpha_{22}v_2$$
$$\vdots$$
$$v_iT=\alpha_{i1}v_1+\alpha_{i2}v_2+\ldots+\alpha_{ii}v_i$$
$$v_nT=\alpha_{n1}v_1+\alpha_{n2}v_2+\ldots+\alpha_{nn}v_n$$

أي إذا كان v_iT تركيبا خطيا لـ v_i والمتجهات السابقة له في الأساس فقط .

مبرهنة (٦-٤-١)

إذا كانت جذور $T\in A(V)$ تقع في F فإنه يوجد أساس لـ V بحيث تكون مصفوفة T مثلثة .

البرهان

باستخدام الاستقراء الرياضي على $\dim_F V$. إذا كان $\dim_F V=1$ فإن كل عنصر في $A(V)$ هو عنصر قياسي ومن ثم فالمبرهنة صحيحة في هذه الحالة .

لنفرض أن المبرهنة صحيحة لجميع فضاءات المتجهات على F التي أبعادها هي $n-1$ وليكن بعد V على F هو n. إن جميع الجذور المميزة للتحويل الخطي T لـ V تقع في F. ليكن $\lambda_1\in F$ جذرًا مميزا لـ T ، عندئذ يوجد متجه غير صفري $v_1\in V$ بحيث يكون $v_1T=\lambda_1 v_1$. ليكن $W=\{\alpha v_1|\alpha\in F\}$. إن W فضاء جزئي من V بعده يساوي 1 كما أنه غير متغير تحت تأثير T. ليكن $\bar{V}=V/W$ ، عندئذ وفقا لتمهيدية (٤-٢-٦)

$$\dim\bar{V}=\dim V-\dim W=n-1$$

ومن تمهيدية (٦-٤-١) نجد أن T يحدث تحويلا خطيا $\bar{T}$ على $\bar{V}$ الذي كثيرة حدوده الدنيا على F تقسم كثيرة الحدود الدنيا لـ T على F. وهكذا فإن جميع جذور كثيرة الحدود الدنيا لـ $\bar{T}$ والتي هي جذور لكثيرة الحدود الدنيا لـ T يجب أن تقع في F. إن التحويل الخطي $\bar{T}$ بتأثيره على $\bar{V}$ يحقق فرضية المبرهنة، ولما كان بعد $\bar{V}$ على F يساوي $n-1$ ، لذا فإنه من فرضية الاستقراء يوجد أساس $\bar{v}_2,\bar{v}_3,\ldots,\bar{v}_n$ لـ $\bar{V}$ على F بحيث يكون

$$..\bar{v}_2\bar{T}=\alpha_{22}\bar{v}_2$$

$$..\bar{v}_3\bar{T}=\alpha_{32}\bar{v}_2+\alpha_{33}\bar{v}_3$$

$$\vdots$$

$$..\bar{v}_i\bar{T}=\alpha_{i2}\bar{v}_2+\alpha_{i3}\bar{v}_3+\ldots+\alpha_{ii}\bar{v}_i$$

$$\vdots$$

$$..\bar{v}_n\bar{T}=\alpha_{n2}\bar{v}_2+\alpha_{n3}\bar{v}_3+\ldots+\alpha_{nn}\bar{v}_n$$

لتكن $v_2,\ldots,v_n$ هي العناصر من V التي تُصَوَّر إلى $\bar{v}_2,\ldots,\bar{v}_n$ على الترتيب. عندئذ فإن $v_1,v_2,\ldots,v_n$ تؤلف أساسا لـ V (انظر مسألة ٣ في نهاية هذا البند). وبما أن $\bar{v}_2\bar{T}=\alpha_{22}\bar{v}_2$. لذا فإن $\bar{v}_2\bar{T}-\alpha_{22}\bar{v}_2=0$. وبالتالي فإن $v_2T-\alpha_{22}v_2\in W$ وهكذا فإن $v_2T-\alpha_{22}v_2$ مضاعف لـ v_1. أي أن $v_2T-\alpha_{22}v_2=\alpha_{21}v_1$ مما ينتج عنه أن $v_2T=\alpha_{21}v_1+\alpha_{22}v_2$ وبالمثل فإن: $v_iT-\alpha_{i2}v_2-\alpha_{i3}v_3-\ldots-\alpha_{ii}v_i\in W$ ومن ثم فإن: $v_iT=\alpha_{i1}v_1+\alpha_{i2}v_2+\ldots+\alpha_{ii}v_i$. إن الأساس $v_1,\ldots,v_n$ لـ V على F يزودنا بأساس يكون فيه v_iT تركيبًا خطيًا لـ v_i وسوابقه وبالتالي فإن مصفوفة T بالنسبة لهذا الأساس مثلثة مما ينهي الاستقراء ومن ثم ينتهي البرهان.

الآن نود صياغة المبرهنة (٦-٤-١) في حالة المصفوفات. لنفرض الآن أن جميع الجذور المميزة للمصفوفة $A\in F_n$ تقع في F. إن A تعرف تحويلاً خطيًا T على $F^{(n)}$ الذي مصفوفته بالنسبة للأساس

$$v_1=(1,0,\ldots0),\ v_2=(0,1,0,\ldots,0),\ \ldots,\ v_n=(0,\ldots,0,1)$$

هي A تماما. إن الجذور المميزة لـ T التي تساوي الجذور المميزة لـ A جميعها تقع في F، ومن ثم فإنه وفقا لمبرهنة (٦-٤-١) يوجد أساس لـ $F^{(n)}$ بحيث تكون مصفوفة T مثلثة. ورغم ذلك واستنادًا إلى مبرهنة (٦-٣-٢) فإن تغيير الأساس هذا بدوره يغير مصفوفة T، أي A، بالنسبة للأساس الأول إلى CAC^{-1}، حيث $C\in F_n$. وهكذا نحصل على صيغة بديلة لمبرهنة (٦-٤-١) كما يلي:

صيغة بديلة لمبرهنة (٦-٤-١)

إذا كانت جميع الجذور المميزة للمصفوفة $A\in F_n$ تقع في F فإنه توجد مصفوفة $C\in F_n$ بحيث تكون CAC^{-1} مصفوفة مثلثة.

يمكن وصف مبرهنة (٦-٤-١) (في أي من صيغتيها) بالقول بأنه يمكن تحويل T (أو A) إلى الصيغة المثلثة على F. إذا نظرنا إلى المسألة (٢٨) في نهاية البند (٦-٣)، فإننا نرى أنه بعد تحويل T إلى الصيغة المثلثة أن العناصر في القطر الرئيس من

مصفوفته تلعب القاعدة المهمة الآتية وهي أن هذه العناصر هي بالفعل الجذور المميزة لـ T.

ونختتم هذا البند بالمبرهنة الآتية:

مبرهنة (٦-٤-٢)

إذا كان بعد V على F هو n ، وإذا كانت جميع الجذور المميزة لـ $T \in A(V)$ تقع في F ، فإن T يحقق كثيرة حدود درجتها n على F.

البرهان

وفقا لمبرهنة (٦-٤-١) نستطيع إيجاد أساس $v_1,\ldots,v_n$ لـ V على F بحيث يكون

$$v_1T=\lambda_1v_1$$
$$v_2T=\alpha_{21}v_1+\lambda_2v_2$$
$$\vdots$$
$$v_iT=\alpha_{i1}v_1+\ldots+\alpha_{i,i-1}v_{i-1}+\lambda_iv_i$$

حيث $i=1,2,\ldots,n$.

وبعبارة أخرى

$$v_1(T-\lambda_1)=0$$
$$v_2(T-\lambda_2)=\alpha_{21}v_1$$
$$\vdots$$
$$v_i(T-\lambda_i)=\alpha_{i1}v_1+\ldots+\alpha_{i,i-1}v_{i-1}$$

حيث $i=1,2,\ldots,n$.

الآن ما هو العنصر $v_2(T-\lambda_2)(T-\lambda_1)$ ؟ لما كان $v_2(T-\lambda_2)=\alpha_{21}v_1$ و $v_1(T-\lambda_1)=0$ ، فإننا نحصل على $v_2(T-\lambda_2)(T-\lambda_1)=0$. ولما كان $(T-\lambda_2)(T-\lambda_1)=(T-\lambda_1)(T-\lambda_2)$ فإن $v_1(T-\lambda_2)(T-\lambda_1)=v_1(T-\lambda_1)(T-\lambda_2)=0$.

وبالاستمرار بهذا النوع من الحسابات نحصل على:

$$v_1(T-\lambda_i)(T-\lambda_{i-1})\ldots(T-\lambda_1)=0$$

$$v_2(T-\lambda_i)(T-\lambda_{i-1})\ldots(T-\lambda_1)=0$$

$$\vdots$$

$$v_i(T-\lambda_i)(T-\lambda_{i-1})\ldots(T-\lambda_1)=0$$

وإذا كانت $i=n$ فإن المصفوفة :

$$S=(T-\lambda_n)(T-\lambda_{n-1})\ \ldots\ (T-\lambda_1)$$

تحقق العلاقة

$$v_1S=v_2S=\ldots=v_nS=0$$

وعندئذ لما كانت S تُفْني أساس V لذلك فإنها يجب أن تُفْني جميع V. وبالتالي فإن $S=0$ وبناء عليه فإن T تحققَ كثيرة الحدود $(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_n)\in F[x]$ من الدرجة n مثبتين بذلك المبرهنة.

ومن طبيعة الأمور، ولسوء الحظ، لا يشترط أن تقع جميع الجذور المميزة لأي تحويل خطي على فضاء متجهات على حقل F في ذلك الحقل F. إن هذا يعتمد تماما على الحقل F. وعلى سبيل المثال، إذا كان F هو حقل الأعداد الحقيقية فإن كثيرة الحدود الدنيا للمصفوفة

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

على F هي $x^2+1=0$ التي ليست لها جذور في F. وعلى ذلك فإنه ليس من حقنا أن نفترض أن الجـذور المميزة تقـع دائما في الحقل المفروض في السؤال. ومع ذلك، نسأل هل بإمكـاننـا تمديد الحقل F إلى حقل جديد K بحيث أن K يحوي جميع الجذور المميزة للمصفوفة أو التحويل الخطي؟

سنناقش هذا في حالـة المصفـوفات، ويمكن عمل شيء مشابه تماما بالنسبة للتحويلات الخطية. إن ما نحتاجه هو الآتي: إذا كان لدينا فضاء متجهات V بعده على حقـل F هو n وكـان K امتـدادًا لـ F فإننا نستطيع إدخال V في فضاء متجهات

V_K على K كما أن بعده على K هو n. إن إحدى الطرق لإنجاز هذا هي أن نأخذ الأساس $v_1,\dots,v_n$ لـ V على F ثم نعتبر V_K على أنه مجموعة التركيبات الخطية $\alpha_1v_1+\dots+\alpha_nv_n$ حيث $\alpha_i\in K$ معتبرين أن v_i مستقلة خطيا على K. إن هذا الاستعمال المكثف للأساس غير ضروري إذ يمكن عمل الشيء نفسه وذلك بإدخال مفهوم الضرب الممتد لفضاءات المتجهات بيد أننا لن نستعمله هنا. وبدلا من ذلك فإننا سنستعين بالمصفوفات (وهو، بالفعل، الشيء الذي اتبعناه آنفا باستخدام أساس ثابت لـ V).

لنعتبر الجبر F_n. إذا كان K هي أي امتداد لـ F فإن $F_n\subset K_n$ حيث K_n هو مجموعة المصفوفات من النوع n×n على K وبالتالي فإن أية مصفوفة على F يمكن اعتبارها مصفوفة على K. فإذا كانت p (x) هي كثيرة الحدود الدنيا لـ $T\in F_n$ على F وباعتبار T عنصرا من K_n فإن من الممكن أن يحقق T كثيرة حدود مختلفة $p_0(x)$ على K. وعندئذ فإن $p_0(x)|p(x)$ لأن $p_0(x)$ يقسم جميع كثيرات الحدود على K (ومن ثم جميع كثيرات الحدود على F) التي يحققها T. الآن نعين K ، فاستنادا إلى مبرهنة (٥-٣-٢) يوجد امتداد منته K لـ F بحيث توجد فيه جميع جذور كثيرة الحدود الدنيا p(x) لـ T على F. باعتبار T عنصرًا من K_n (ومن أجل K نفسه) هل توجد جميع جذور T المميزة في K ؟ والجواب على ذلك، وباعتبار T عنصرًا من K_n فإن كثيرة الحدود الدنيا $p_0(x)$ لـ T على K تقسم p(x) وبالتالي فإن جميع جذور $p_0(x)$ هي جذور لـ p(x) ومن ثم فإنها تقع في K. وبالتالي وباعتبار T عنصرًا من K_n فإن جميع جذوره المميزة تقع في K.

وهكذا، إذا كان $T\in F_n$ فإن بالرجوع إلى حقل الانشطار K لكثيرة الحدود الدنيا يمكن التحقق من فرضيات مبرهنتي (٦-٤-١) و (٦-٤-٢) ليس فقط على F بل أيضا على K. ومن أجل ذلك، وعلى سبيل المثال، فإنه يمكن تحويل T إلى الصيغة المثلثة على K، كما أنها تحقق كثيرة حدود درجتها n على K . أحيانا، وعندما يحالفنا الحظ، فإن معرفة نتيجة صحيحة على K تجعلنا نستنتج أن تلك النتيجة صحيحة بالنسبة لـ F . ورغم ذلك فإن استخدام K ليس هو العلاج الأمثل إذ أنه توجد حالات كثيرة تكون

فيها النتائج في K غير مفيدة في F. وهذا هو السبب في وجود نوعين من مبرهنات الصيغ القانونية: أحدهما هو الذي نفترض فيه أن جميع الجذور المميزة لـ T تقع في F، والآخر هو ذلك الذي لا يحقق هذا الشرط.

كلمة أخيرة، إذا كانت $T \in F_n$ فإننا نعني بالعبارة «**الجذر المميز لـ T**» العنصر λ في حقل الانشطار K لكثيرة الحدود الدنيا $p(x)$ لـ T على F، بحيث لا يوجد لـ $\lambda - T$ معكوس في K_n. وفي الحقيقة إن كل جذر لكثيرة الحدود الدنيا لـ T على F هو جذر مميز لـ T (انظر مسألة ٥).

مسائل

١ - برهن على أن علاقة التشابه هي علاقة تكافؤ على $A(V)$.

٢ - إذا كانت $T \in F_n$ وكان $K \supset F$. فأثبت أنه يوجد معكوس لـ T وذلك باعتبارها عنصرًا من K_n إذا وفقط إذا كان لها معكوس في F_n.

٣ - أثبت أن المتجهات $v_1, \ldots, v_n$ الواردة في برهان مبرهنة (٦-٤-١) هي أساس لـ V.

٤ - برهن باستخدام المصفوفات على أنه إذا كانت A مصفوفة مثلثة من النوع $n \times n$ وكانت العناصر في القطر الرئيس هي $\lambda_1, \ldots, \lambda_n$ فإن

$$(A-\lambda_1)(A-\lambda_2)\ldots(A-\lambda_n)=0$$

٥* - إذا كانت كثيرة الحدود الدنيا لـ T في F_n هي $p(x)$. فأثبت أن أي جذر في حقل انشطاره K هو جذر مميز لـ T.

٦ - إذا كان $T \in A(V)$ وكان $\lambda \in F$ جذرا مميزا لـ T في F وإذا كان $V_\lambda = \{v \in V \mid vT = \lambda v\}$ وكان $S \in A(V)$ يتبادل مع T. فأثبت أن V_λ غير متغير تحت تأثير S.

٧* - إذا كانت $\mathcal{M}$ مجموعة إبدالية من العناصر في $A(V)$ بحيث تكون جميع جذور $M \in \mathcal{M}$ المميزة في F. فأثبت أنه يوجد $C \in A(V)$ بحيث يكون CMC^{-1}، $M \in \mathcal{M}$ في الصيغة المثلثة وذلك لكل M في $\mathcal{M}$.

٨ ـ ليكن W فضاءً جزئيًا غير متغير تحت تأثير $T\in A(V)$. وبقصر T على W فإن T يحدث تحويلاً خطيًا $\tilde{T}$.. (معرفا بالقاعدة $w\tilde{T}=wT$ لكل $w\in W$) ولتكن $\tilde{p}$.. هي كثير الحدود الدنيا لـ $\tilde{T}$ على F.

(ا) أثبت أن $\tilde{p}(x)|p(x)$. حيث $p(x)$ هي كثيرة الحدود الدنيا لـ T على F.

(ب) إذا كان T يحدث $\bar{T}$ على V/W وكان $\bar{T}$ يحقق كثيرة حدود دنيا $\bar{p}(x)$. على F فأثبت أن $p(x)|\tilde{p}(x)\bar{p}(x)$.

(جـ)* إذا كان $\tilde{p}(x)$. و $\bar{p}(x)$. أوليين نسبيا فبرهن على أن $p(x)=\tilde{p}(x)\bar{p}(x)$.

(د)* أورد مثالا لـ T يكون فيه $p(x)\neq\tilde{p}(x)\bar{p}(x)$.

٩ ـ لتكن $\mathcal{M}$ مجموعة غير خالية من العناصر في $A(V)$. يقال عن الفضاء الجزئي W من V إنه *غير متغير تحت تأثير* $\mathcal{M}$ إذا كان $WM\subset W$ لكل $M\in\mathcal{M}$. إذا كان W غير متغير تحت تأثير $\mathcal{M}$ وكان بعده على F هو r. فأثبت أنه يوجد أساس لـ V على F بحيث يكون لكل $M\in\mathcal{M}$ مصفوفة بالنسبة لهذا الأساس من الصيغة

$$\left(\begin{array}{c|c} M_1 & 0 \\ \hline M_{12} & M_2 \end{array}\right)$$

حيث M_1 مصفوفة من النوع $r\times r$ ، M_2 مصفوفة من النوع $(n-r)\times(n-r)$.

١٠ ـ في المسألة (٩). أثبت أن M_1 هي مصفوفة التحويل الخطي $\tilde{M}$ المحدث بوساطة M على W كما أن M_2 هي مصفوفة التحويل الخطي $\bar{M}$.. المحدث بواسطة M على V/W.

١١* ـ يقال عن المجموعة غير الخالية $\mathcal{M}$ من التحويلات الخطية في $A(V)$ إنها مجموعة *غير مختزلة* إذا كانت الفضاءات الجزئية غير المتغيرة تحت تأثير $\mathcal{M}$ في V هي (0) و V فقط. إذا كانت $\mathcal{M}$ مجموعة غير مختزلة من التحويلات الخطية على V وكان

$$D=\{T\in A(V)|TM=MT \text{ ، لكل } M\in\mathcal{M}\}$$

فأثبت أن D حلقة قسمة.

١٢*ـ حل المسألة (١١) بالاستعانة بمسألة (١٤) (تمهيدية شور) الواردة في نهاية الفصل الرابع.

١٣*- إذا كان F يحقق الخاصة التي تنص على أن جميع الجذور المميزة لجميع العناصر في A(V) تقع في F. فأثبت أن D الواردة في المسألة (١١) تتكون فقط من القياسيات.

١٤ - ليكن F هو حقل الأعداد الحقيقية ولتكن

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in F_2$$

(أ) برهن على أن المجموعة المكونة فقط من $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ هي مجموعة غير مختزلة.

(ب) أوجد مجموعة المصفوفات D التي تتبادل مع $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ثم أثبت أن D تماثل حقل الأعداد المركبة.

١٥ - ليكن F هو حقل الأعداد الحقيقية.

(أ) برهن على أن المجموعة

$$\mathcal{M}=\left\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}\right\}$$

هي مجموعة غير مختزلة

(ب) أوجد جميع المصفوفات $A \in F_4$ بحيث أن $MA=AM$ لكل $M \in \mathcal{M}$

(جـ) برهن على أن مجموعة المصفوفات A الواردة في (ب) هي حلقة قسمة تماثل حلقة قسمة الرباعيات على حقل الأعداد الحقيقية.

١٦ - يقال عن مجموعة التحويلات الخطية $\mathcal{M} \subset A(V)$ إلا أنها *قابلة للتفريق* إذا كان يوجد فضاء جزئي $W \subset V$ بحيث يكون $V=W \oplus W_1$ حيث $W \neq 0$ و $W \neq V$ كما أن كلا من W أو W_1 غير متغير تحت تأثير $\mathcal{M}$. وإذا لم يتحقق الشرط السابق فإنه يقال عنها إنها غير *قابلة للتفريق*.

(أ) إذا كانت $\mathcal{M}$ مجموعة قابلة للتفريق من التحويلات الخطية على V. فأثبت أنه يوجد أساس لـ V بحيث تكون مصفوفة كل عنصر M من $\mathcal{M}$ من الشكل

$$\left(\begin{array}{c|c} M_1 & 0 \\ \hline 0 & M_2 \end{array}\right)$$

حيث M_1 ، M_2 مصفوفات مربعة .

(ب) إذا كان V فضاء متجهات بعده على F هو n وكان $T\in A(V)$ يحقق العلاقة $T^n=0$ وكذلك $T^{n-1}\neq 0$. فأثبت أن المجموعة $\{T\}$ (المكونة من T فقط) غير قابلة للتفريق .

١٧ ـ ليكن $T\in A(V)$ ولتكن $p(x)$ هي كثيرة حدود T الدنيا على F

(ا) إذا كانت $p(x)$ تقبل القسمة على كثيرتي حدود غير مختزلتين $p_1(x)$ و $p_2(x)$ في $F[x]$ فاثبت أن $\{T\}$ قابلة للتفريق .

(ب) إذا كانت $\{T\}$ غير قابلة للتفريق ، حيث $T\in A(V)$. فأثبت أن كثيرة الحدود الدنيا لـ T على F هي قوة لكثيرة حدود غير مختزلة .

١٨ ـ إذا كان $T\in A(V)$ معدوم القوى . فأثبت أنه يمكن تحويل T إلى الصيغة المثلثة على F ، كما أن جميع العناصر في القطر الرئيس في تلك الصيغة أصفارًا .

١٩ ـ إذا كانت جذور $T\in A(V)$ المميزة تتكون فقط من الصفر . فأثبت أن T معدوم القوى .

(٦ـ٥) الصيغ القانونية : التحويلات معدومة القوى

إن أحد أنواع التحويلات الخطية التي جميع جذورها المميزة تقع في F هو نوع التحويلات الخطية المعدومة القوى لأن جميع جذورها المميزة أصفار ومن ثم فإنها تقع في F. وبناءً على ذلك ، فإنه وفقا لنتائج البند السابق يمكن تحويل أي تحويل خطي معدوم القوى إلى الصيغة المثلثة على F دائما . إن هذا ليس دقيقا بصورة كافية ولكننا سنتحدث عنه على نطاق أوسع .

وعلى الرغم من أن التحويلات الخطية معدومة القوى محدودة بعض الشيء إلا أنها تستحق الدراسة . والحقيقة أنه متى ما وجدنا صيغة قانونية مناسبة لهذه التحويلات فإننا نستطيع إيجاد صيغة قانونية مناسبة لجميع التحويلات الخطية التي جذورها المميزة تقع في F .

الآن نبحث الـطريقة التي سنتبعها لمعالجة الموضوع. إننا نستطيع دراسة هذه الأمور من منطلق أولي أو بإمكاننا استغلال نتائج تفريق الفضاءات الحلقية التي حصلنا عليها في الفصل الرابع ولقد قررنا أن نسلك طريقًا وسطًا بين الأمرين، وسنعالج المادة في هذا البند والذي يليه (صيغ جوردان) دون التطرق إلى الفضاءات الحلقية ونتائجها المطورة في الفصل الرابع. ومع ذلك فإننا سنغير وجهة النظر تماما وذلك في البند الذي يعـالـج الصيغ القانونية النسبية وسنقدم عبر التحويل الخطي بناء فضاء حلقي على فضاءات المتجهات التي تحت الدراسة مستخدمين بذلك مبرهنة (٤-٥-١) وسنحصل على تفريق لفضاء المتجهات والصيغة القانونية الناتجة وذلك بالنسبة لتحويل خطي معين.

وعلى الرغم من أننا لن نستخدم المنطلق النظري للفضاء الحلقي الآن إلا أن على القارىء ملاحظة التشابه في المناقشة الواردة في برهان (٤-٥-١) وتلك الواردة في تمهيدية (٦-٥-٤).

وقبل أن نركز جهودنا على التحويلات الخطية المعدومة القوى فإننا نبرهن نتيجة مهمة وسارية المفعول لتحويلات خطية عامة.

تمهيدية (٦-٥-١)

إذا كان $V=V_1\oplus V_2\oplus\ldots\oplus V_k$ حيث إن بعد كل من V_i هو n_i كما أن V_i غير متغير تحت تأثير $T\in A(V)$ ، لكل i. عندئذ يمكن إيجاد أساس لـ V بحيث تأخذ مصفوفة T بالنسبة لهذا الأساس الشكل

$$\begin{pmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & A_k \end{pmatrix}$$

حيث A_i مصفوفة من النوع $n_i\times n_i$ كما أن A_i هي مصفوفة التحويل الخطي المحدث من قبل T على V_i.

البرهان

لنختار أساس V كما يلي : $v_1^{(1)},\dots,v_{n_1}^{(1)}$ هو أساس V_1 و $v_1^{(2)},\dots,v_{n_2}^{(2)}$ هو أساس V_2 وهكذا. ولما كان كل من V_i غير متغير تحت تأثير T ، لذا فإن $v_j^{(i)}T\in V_i$ وبالتالي فإنه تركيب خطي للأساس $v_1^{(i)},v_2^{(i)},\dots,v_{n_i}^{(i)}$ وبالتالي فإنه يمكن اختيار مصفوفة T بالنسبة لهذا الأساس لتأخذ الصيغة المطلوبة. إن كون A_i هي مصفوفة T_i الذي هو التحويل الخطي المحدث بواسطة T على V_i واضح من تعريف مصفوفة التحويل الخطي.

الآن نحصر اهتمامنا على التحويلات الخطية المعدومة القوى.

تمهيدية (٦-٥-٢)

إذا كان $T\in A(V)$ معدوم القوى فإن للتحويل الخطي $\alpha_0+\alpha_1T+\dots+\alpha_nT^n$ معكوس إذا كان $\alpha_0\neq 0$ ، حيث $a_i\in F$.

البرهان

إذا كان S معدوم القوى و $0\neq\alpha_0\in F$ فإن حسابا بسيطا يثبت أن

$$(\alpha_0+S)\left(\frac{1}{\alpha_0}-\frac{S}{\alpha_0^2}+\frac{S^2}{\alpha_0^3}+\dots+(-1)^{r-1}\frac{S^{r-1}}{\alpha_0^r}\right)=1$$

وذلك إذا كان $S^r=0$. لكن إذا كان $T^r=0$ فإن

$$S=\alpha_1T+\alpha_2T^2+\dots+\alpha_mT^m$$

يجب أن يحقق الشرط $S^r=0$ (أثبت ذلك). وبالتالي إذا كان $0\neq\alpha_0\in F$ فإن لـ α_0+S معكوس.

اصطــلاح

سنرمز بـ M_t للمصفوفة من النوع $t\times t$ من الشكل

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 0 & 0 & & \dots & 0 & 1 \\ 0 & 0 & & \dots & 0 & 0 \end{pmatrix}$$

والتي جميع عناصرها أصفار سوى تلك العناصر في القطر فوق الرئيس حيث كل منها يساوي 1.

تعريف

إذا كان $T \in A(V)$ معدوم القوى فإن العدد k يسمى دليل انعدام القوى (index of nilpotence) لـ T إذا كان $T^k=0$ ولكن $T^{k-1}\neq 0$.

إن النتيجة الرئيسة للتحويلات الخطية المعدومة القوى هي المبرهنة التالية.

مبرهنة (٦-٥-١)

إذا كان $T \in A(V)$ معدوم القوى وكان دليل انعدام قوى T هو n_1 فإنه يمكن إيجاد أساس لـ V بحيث تأخذ مصفوفة T بالنسبة لهذا الأساس الصيغة الآتية:

$$\begin{pmatrix} M_{n_1} & & & \\ & M_{n_2} & & \\ & & \ddots & \\ & & & M_{n_r} \end{pmatrix}$$

حيث $n_1 \geqslant n_2 \geqslant \ldots \geqslant n_r$ كما أن $n_1+n_2+\ldots+n_r=\dim_F V$

البرهان

سيكون البرهان مفصلا إلى حد ما، وكلما تقدمنا فيه فإننا سنجعل بعض فقراته على شكل تمهيديات.

لما كان $T^{n_1}=0$ وكان $T^{n_1-1}\neq 0$، لذا فإنه يمكن إيجاد متجه $v \in V$ بحيث يكون $vT^{n_1-1}\neq 0$. إن المتجهات $v, vT, \ldots, vT^{n_1-1}$ مستقلة خطيا على F. ولإثبات ذلك، لنفرض أن $\alpha_1 v+\alpha_2 vT+\ldots+\alpha_{n_1} vT^{n_1-1}=0$ حيث $\alpha_i \in F$ وليكن α_s هو أول عنصر لا يساوي صفرا، لذلك فإن

$$vT^{s-1}(\alpha_s+\alpha_{s+1}T+\ldots+\alpha_{n_1}T^{n_1-s})=0$$

ولما كان $\alpha_s\neq 0$، لذا فإن للتحويل $\alpha_s+\alpha_{s+1}T\ldots+\alpha_{n_1}T^{n_1-s}$ معكوسا وذلك وفقا لتمهيدية

(٦-٥-٢). وبناء عليه فإن $vT^{s-1}=0$ ، ومع ذلك، لما كان $s<n_1$ فإن هذا يناقض كون $vT^{n_1-1}\neq 0$. وبالتالي فإنه لا يوجد مثل هذا العدد، أي α_s ، ومن ثم فإن $v,vT,\ldots,vT^{n_1-1}$ مستقلة خطيا على F.

ليكن V_1 هو الفضاء الجزئي من V المولد بالعناصر $v_1=v,v_2=vT,\ldots,v_{n_1}=vT^{n_1-1}$ عندئذ V_1 غير متغير تحت تأثير T. وعندئذ فإن مصفوفة التحويل الخطي المحدث بواسطة T على V_1 بالنسبة للأساس المذكور آنفا هي M_{n_1}.

لقد حصلنا حتى الآن على الجزء الأيسر الأعلى من المصفوفة الواردة في المبرهنة ويجب أن نحصل على بقية هذه المصفوفة.

تمهيدية (٦-٥-٣)

إذا كان $u\in V_1$ يحقق الشرط $uT^{n_1-k}=0$ حيث $0<k\leq n_1$ فإن $u=u_0T^k$ حيث u_0 عنصر من V_1.

البرهان

لما كان $u\in V_1$ لذا فإن:

$$u=\alpha_1 v+\alpha_2 vT+\ldots+\alpha_k vT^{k-1}+\alpha_{k+1}vT^k+\ldots+\alpha_{n_1}vT^{n_1-1}$$

وعليه فإن

$$0=uT^{n_1-k}=\alpha_1 vT^{n_1-k}+\ldots+\alpha_k vT^{n_1-1}$$

ولكن $vT^{n_1-k},\ldots,vT^{n_1-1}$ مستقلة خطيا على F لذا $\alpha_1=\alpha_2=\ldots=\alpha_k=0$ وعليه فإن $u=\alpha_{k+1}vT^k+\ldots+\alpha_{n_1}vT^{n_1-1}=u_0T^k$ ، حيث $u_0=\alpha_{k+1}v+\ldots+\alpha_{n_1}vT^{n_1-k-1}\in V_1$.

إن المناقشة حتى هذه اللحظة كانت مباشرة إلى حد ما بيد أنها ستصبح الآن أكثر تعقيدا.

تمهيدية (٦-٥-٤)

يوجد فضاء جزئي W من V غير متغير تحت تأثير T بحيث يكون $V=V_1\oplus W$.

البرهان .

ليكن W هو الفضاء الجزئي من V الذي بعده أكبر ما يمكن بحيث يكون:

(ا) $V_1 \cap W = (0)$

(ب) W غير متغير تحت تأثير T.

ونريد إثبات أن $V = V_1 + W$. لنفرض خلاف ذلك، عندئذ يوجد عنصر $z \in V$ بحيث يكون $z \notin V_1 + W$. وبما أن $T^{n_1} = 0$ ، لذلك فإنه يوجد عدد صحيح k ، $0 < k \leq n_1$ بحيث يكون $zT^k \in V_1 + W$ كما أن $zT^i \notin V_1 + W$ حيث $i < k$. وهكذا نجد أن $zT^k = u + w$ ، حيث $u \in V_1$ و $w \in W$ ولكن عندئذ

$$0 = zT^{n_1} = (zT^k)(T^{n_1-k}) = uT^{n_1-k} + wT^{n_1-k}$$

ومع ذلك، ولكون كل من V_1 ، W غير متغير تحت تأثير T ، فإن $uT^{n_1-k} \in V_1$ و $wT^{n_1-k} \in W$. وبما أن $V_1 \cap W = (0)$ ، فإن هذا يقتضي أن $uT^{n_1-k} = -wT^{n_1-k} \in V_1 \cap W = (0)$ الأمر الذي ينتج عنه أن $uT^{n_1-k} = 0$ ووفقا لتمهيدية (٦ـ٥ـ٣) فإن $u = u_0T^k$ حيث $u_0 \in V_1$ ، ومن أجل ذلك $zT^k = u + w = u_0T^k + w$. ليكن $z_1 = z - u_0$ ، عندئذ $z_1T^k = zT^k - u_0T^k = w \in W$. ولما كان W غير متغير تحت تأثير T لذا فإن هذا يقتضى أن $z_1T^m \in W$ لكل $m \geq k$. ومن ناحية أخرى، إذا كان $i < k$ فإن $z_1T^i = zT^i - u_0T^i \notin V_1 + W$ ، لأنه خلاف ذلك، يجب أن يكون zT^i في $V_1 + W$ مما يناقض اختيار k.

ليكن W_1 هو الفضاء الجزئي من V المولد بـ W والمتجهات $z_1, z_1T, \ldots, z_1T^{k-1}$ وحيث إن $z_1 \notin W$ و $W_1 \supset W$ لذلك فإن بعد W_1 يجب أن يكون أكبر من بعد W. وفضلا عن ذلك، بما أن $z_1T^k \in W$ وبما أن W غير متغير تحت تأثير T لذلك فإن W_1 يجب أن يكون غير متغير تحت تأثير T. ووفقا لطبيعة W الأعظمية، فإنه يجب أن يوجد عنصر في $W_1 \cap V_1$ من الصيغة $w_0 + \alpha_1 z_1 + \alpha_2 z_1 T + \ldots + \alpha_k z_1 T^{k-1} \neq 0$ ، حيث $w_0 \in W$. إن العناصر $\alpha_1, \ldots, \alpha_k$ ليست كلها أصفارًا لأنه خلاف ذلك يكون لدينا $0 \neq w_0 \in W \cap V_1 = (0)$ وهذا تناقض. ليكن α_s هو أول عنصر في $\alpha_1 \ldots \alpha_k$ الذي لا يساوي صفرا عندئذ

$$w_0 + z_1 T^{s-1}(\alpha_s + \alpha_{s+1} T + \ldots + \alpha_k T^{k-s}) \in V_1$$

وحيث إن $\alpha_s \neq 0$ ، لذا فإنه وفقا لتمهيدية (٦ـ٥ـ٢) يجب أن يوجد لـ $a_s + \alpha_{s+1} T + \ldots + \alpha_k T^{k-s}$ معكوس، كما أن معكوسه، R ، هي كثيرة حدود في T. وهكذا

فإن كلا من V_1,W غير متغير تحت تأثير R ، ومع ذلك، فإننا نجد مما ورد آنفا أن $w_0R+z_1T^{s-1}\in V_1R\subset V_1$ ، مما يقتضي أن $z_1T^{s-1}\in W_1+WR\subset V_1+W$. ولما كان $s-1<k$ فإن هذا مستحيل ومن أجل ذلك فإن $V_1+W=V$. وحيث إن $V_1\cap W=(0)$ لذلك فإن $V=V_1\oplus W$ وبهذا ينتهي برهان التمهيدية.

إن الجهـــد الأكبر قد انتهى إلى حـد الآن. والآن نكمـــل برهـان مبرهنة (٦ - ٥ - ١).

استنادا إلى تمهيدية (٦ - ٥ - ٤) فإن $V=V_1\oplus W$ ، حيث W غير متغير تحت تأثير T. باستخدام الأساس $v_1,\ldots,v_{n_1}$ لـ V_1 وأي أساس لـ W ليكون أساسا لـ V ووفقا لتمهيدية (٦ـ٥ـ١) فإن مصفوفة T تأخذ الشكل

$$\begin{pmatrix} M_{n_1} & 0 \\ 0 & A_2 \end{pmatrix}$$

حيث A_2 هي مصفوفة T_2 التحويل الخطي المحدث على W بواسطة T. وبما أن $T^{n_1}=0$. لذا فإن $T_2^{n_2}=0$ حيث $n_2\leq n_1$. وبتكـرار المنـاقشة المستخدمة حول T على V من أجل T_2 على W يمكننا تفريق W ، كما فعلنا من أجل V (أو باستخدام الاستقراء على بعد فضاء المتجهات المدروس) والاستمرار بهذه الطريقة نحصل على أساس لـ V بحيث تأخذ مصفوفة T الشكل

$$\begin{pmatrix} M_{n_1} & 0 & \ldots & 0 \\ 0 & M_{n_2} & & \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & M_{n_r} \end{pmatrix}$$

إن المساواة $n_1+n_2+\ldots+n_r=\dim_F V$ واضحة ذلك أن سعة المصفوفة هو $n\times n$ حيث $n=\dim_F V$.

تعريف

يطلق على الأعداد الصحيحة $n_1,n_2,\ldots,n_r$ لا متغيرات T.

تعريف

إذا كان $T\in A(V)$ معدوم القوة فإن الفضاء الجزئي M من V الذي بعده m وغير المتغير تحت تأثير T يسمى دوريا بالنسبة إلى T إذا كان

١) $MT^{m}=(0)$, $MT^{m-1}\neq 0$

٢) يوجد عنصر $z\in M$ بحيث يكون $z,zT,\ldots,zT^{m-1}$ أساس لـ M

(ملاحظة: إن الشرط الثاني يقتضي الشرط الأول).

تمهيدية (٦ـ٥ـ٥)

إذا كان بعد M هو m وكان M دوريا بالنسبة لـ T فإن بعد MT^k هو $m-k$ لكل $k\leq m$.

البرهان

يمكن الحصول على أساس MT^k، وذلك بأخذ صورة أي أساس لـ M تحت تأثير T^k، لذلك باستخدام أساس M الذي هو $z,zT,\ldots,zT^{m-1}$ نحصل على أساس لـ MT^k هو $zT^k,zT^{k+1},\ldots,zT^{m-1}$. وحيث إن هذا الأساس يحتوي على $m-k$ عنصرًا، لذلك فإننا قد برهنا التمهيدية.

إن مبرهنة (٦ـ٥ـ١) تفيد بأنه إذا كان لدينا تحويل خطي معدوم القوى T في $A(V)$، فإننا نستطيع إيجاد أعداد صحيحة $n_1\geqslant n_2\geqslant\ldots\geqslant n_r$ وفضاءات جزئية $V_1,\ldots,V_r$ من V دورية بالنسبة إلى T أبعادها هي $n_1,n_2,\ldots,n_r$ على الترتيب بحيث يكون

$$V=V_1\oplus V_2\oplus\ldots\oplus V_r$$

هل بالإمكان إيجاد أعداد صحيحة أخرى $m_1\geqslant m_2\geqslant\ldots\geqslant m_s$ وفضاءات جزئية $U_1,\ldots,U_s$ من V دورية بالنسبة إلى T وأبعادها على الترتيب هي $m_1,m_2,\ldots,m_s$ بحيث يكون $V=U_1+\ldots+U_s$؟ إننا ندَّعي أن هذا غير ممكن، أو بعبارة أخرى، $r=s$ و $m_1=n_1,\ldots,m_r=n_r$. لنفرض أن هذه ليست هي الحالة، عندئذ يوجد عدد صحيح i بحيث يكون $m_i\neq n_i$. يمكن أن نفرض أن $m_i<n_i$.

لنعتبر VT^{m_i}. بما أنه، من ناحية، $V=V_1\oplus\ldots\oplus V_r$ فإن

$$VT^{m_i}=V_1T^{m_i}\oplus\ldots\oplus V_iT^{m_i}\oplus\ldots\oplus V_rT^{m_i}$$

وبما أن $\dim V_1T^{m_i}=n_1-m_i$ و $\dim V_2T^{m_i}=n_2-m_i,\ldots, \dim V_iT^{m_i}=n_i-m_i$ (وفقا لتمهيدية ٦-٥-٥) لذلك فإن

$$\dim VT^{m}\geqslant(n_1-m_i)+(n_2-m_i)+\ldots+(n_i-m_i)$$

ومن ناحية أخرى، بما أن $V=U_1\oplus\ldots\oplus U_s$ و $U_jT^{m_i}=(0)$ لكل $j\geqslant i$. لذا فإن

$$VT^{m_i}=U_1T^{m_i}\oplus U_2T^{m_i}\oplus\ldots\oplus U_{i-1}T^{m_i}$$

وبالتالي:

$$\dim VT^{m_i}=(m_1-m_i)+(m_2-m_i)+\ldots+(m_{i-1}-m_i)$$

ووفقا لاختيار i فإن:

$$n_1=m_1,n_2=m_2,\ldots,n_{i-1}=m_{i-1}$$

ومن ثم فإن:

$$\dim VT^{m_i}=(n_1-m_i)+(n_2-m_i)+\ldots+(n_{i-1}-m_i)$$

بيد أن هذا يناقض الحقيقة المثبة أعلاه وهي أن:

$$\dim VT^{m_i}\geqslant(n_1-m_i)+\ldots+(n_{i-1}-m_i)+(n_i-m_i)$$

لأن $n_i-m_i>0$.

لهذا فإنه توجد مجموعة وحيدة من الأعداد الصحيحة $n_1\geqslant n_2\geqslant\ldots\geqslant n_r$ بحيث يكون V هو المجموع المباشر للفضاءات الجزئية الدورية بالنسبة إلى T التي أبعادها هي $n_1,n_2,\ldots,n_r$ على الترتيب *«وبعبارة أخرى، لقد برهنا على أن لا متغيرات T وحيدة»*.

وباستخدام لغة المصفوفات، فإن المناقشة التي انتهت الآن تثبت لنا أنه إذا كان

$$m_1\geqslant m_2\geqslant\ldots\geqslant m_s \quad , \quad n_1\geqslant n_2\geqslant\ldots\geqslant n_r$$

فإن المصفوفتين

$$\begin{pmatrix} M_{n_1} & \ldots & 0 \\ 0 & . & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_{n_r} \end{pmatrix} \quad \text{و} \quad \begin{pmatrix} M_{m_1} & \ldots & 0 \\ 0 & . & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_{m_s} \end{pmatrix}$$

تكونان متشابهتين فقط إذا كان $r=s$ و $n_1=m_1,\ldots,n_r=m_r$

بهذا نكون قد برهنا على الجزء الأصعب من المبرهنة.

مبرهنة (٦-٥-٢)

يكون التحويلان الخطيان المعدوما القوى متشابهين إذا وفقط إذا كان لهما نفس اللامتغيرات.

البرهان

إن المناقشة الواردة قبل المبرهنة تثبت لنا أنه إذا كان للتحويلين الخطيين المعدومي القوى لا متغيرات مختلفة فإنه لا يمكن أن يكونا متشابهين لأن مصفوفتيهما

$$\begin{pmatrix} M_{n_1} & \ldots & 0 \\ . & . & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_{n_r} \end{pmatrix} \quad \text{و} \quad \begin{pmatrix} M_{m_1} & \ldots & 0 \\ . & . & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_{m_s} \end{pmatrix}$$

لا يمكن أن تكونا متشابهتين.

أمـا بالنسبة للاتجاه الآخر، فإنه إذا كان للتحويلين الخطيين المعدومي القوى T و S الـلا متغـيرات $n_1 \geqslant \ldots \geqslant n_s$ نفسهـا. فإنه وفقا لمبرهنة (٦-٥-١) يوجد أساسان لـ V هما $v_1,\ldots,v_n$ و $w_1,\ldots,w_n$ بحيث إن مصفوفة S بالنسبـة إلى $v_1 \ldots v_n$ ومصفوفـة T بالنسبة إلى $w_1,\ldots,w_n$ كل منهما تساوي

$$\begin{pmatrix} M_{n_1} & \ldots & 0 \\ 0 & . & . \\ . & . & . \\ . & . & . \\ 0 & \ldots & M_{n_r} \end{pmatrix}$$

فإذا كان A تحويلا خطيا معرفا على V بالقاعدة $v_iA=w_i$ فإن $S=ATA^{-1}$ (أثبت ذلك، ثم قارن بين هذه المسـألـة ومسألة (٣٢) الواردة في نهاية البند (٦-٣)) ومن ثم فإن S و T متشابهان.

دعنا نحسب، الآن، المثال الآتي: لتكن

$$T=\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in F_3$$

تؤثر على $F^{(3)}$ الذي أساسه هو

$$u_1=(1,0,0),\ u_2=(0,1,0),\ u_3=(0,0,1)$$

وليكن:

$$v_1=u_1,\ v_2=uT=u_2+u_3,\ v_3=u_3$$

إن مصفوفة T بالنسبة لهذا الأساس هي

$$\left(\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & 0 \\ \hline 0 & 0 & 0 \end{array}\right)$$

وعليه فإن لا متغيرات T هي 2 و 1. إذا كانت A هي مصفوفة تغيير الأساس، أي

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

فإن حسابا بسيطا يثبت أن:

$$ATA^{-1}=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ملاحظة أخيرة

إن لا متغيرات T تعين تجزيئا للعدد n الذي هو بعد V ، وبالعكس، إن أي تجزيىء للعدد n ، أي $n=n_1+n_2+\ldots+n_r$ ، $n_1\geqslant n_2\geqslant\ldots\geqslant n_r$ يعين لا متغيرات التحويل الخطي المعدوم القوى

$$\begin{pmatrix} M_{n_1} & \ldots & 0 \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 0 & \ldots & M_{n_r} \end{pmatrix}$$

وهكـذا فإن عدد فصـول التشـابـه المختلفة للمصفوفات المعدومة القوى من النوع $n \times n$ هو تماما $p(n)$ ، أي عدد تجزيئات n.

(٦-٦) الصيغ القانونية : تفريق V (صيغة جوردان)

ليكن V فضـاء متجهـات منتهي البعد على F وليكن T عنصرا ما من $A_F(V)$. ولنفـرض أن V_1 فضـاء جزئي غير متغير تحت تأثير T ، عندئذ فإن T يحدث تحويلا خطيا T_1 على V_1 معرفا كما يلي $uT_1=uT$ لكل $u \in V_1$. فإذا كان لدينا أي كثيرة حدود $q(x) \in F[x]$ فإن التحـويل الخـطي المحدث بواسطة $q(T)$ عـلى V_1 هـو $q(T_1)$ (إن برهان هذا متروك كتمرين). وبصورة خاصة، إذا كان $q(T)=0$ فإن $q(T_1)=0$ وعليه فإن T_1 يحقق أي كثيرة حدود محققة من قبل T على F. ماذا نستطيع أن نقول عن الاتجاه الآخـر؟

تمهيدية (٦-٦-١)

لنفرض أن $V=V_1 \oplus V_2$ ، حيث إن V_1 و V_2 فضاءان جزئيان غير متغيرين تحت تأثـير T. وليكن T_1 و T_2 هما التحويلان الخطيان المحدثان بواسطة T على كل من V_1 و V_2 على الترتيب إذا كانت $p_1(x)$ هي كثيرة حدود T_1 الدنيا على F وكانت $p_2(x)$ هي كثيرة حدود T_2 الدنيا على F فإن كثيرة حدود T الدنيا على F هي المضاعف المشترك الأصغر لكل من $p_1(x)$ و $p_2(x)$.

البرهان

إذا كانت $p(x)$ هي كثـيرة حدود T الدنيا على F ، فإن كلا من $p(T_1)$ و $p(T_2)$ تساوي صفرا وذلك كما رأينا أعلاه ولذلك فإن $p_1(x)|p(x)$ و $p_2(x)|p(x)$ وعـــندئذ فإن المضاعف المشترك الأصغر لكل من $p_1(x)$ و $p_2(x)$، يجب أن يقسم $p(x)$.

ومن ناحية أخرى، لنفرض أن $q(x)$ هي المضاعف المشترك الأصغر لـ $p_1(x)$ و $p_2(x)$ ولنعتبر $q(T)$. بما أن $p_1(x)|q(x)$ فإن $v_1q(T)=v_1q(T_1)=0$ حيث $v_1 \in V_1$ وبالمثل

$v_2q(T)=0$ ، حيث $v_2 \in V_2$. فإذا كان $v \in V$ فإنه يمكن كتابته على الصيغة $v=v_1+v_2$ حيث $v_1 \in V_1$ و $v_2 \in V_2$ الأمر الذي يترتب عليه أن :

$$vq(T)=(v_1+v_2)q(T)=v_1q(T)+v_2q(T)=0$$

وهكذا فإن $q(T)=0$ أي أن T يحقق $q(x)$. وبضم هذا مع الفقرة الأولى يتم البرهان.

نتيجة

إذا كان $V=V_1\oplus...\oplus V_k$ حيث V_i غير متغير تحت تأثير T لكل i. وإذا كانت $p_i(x)$ هي كثيرة حدود T_i الدنيا على F ، حيث T_i هو التحويل الخطي المحدث بواسطة T على V_i ، عندئذ فإن كثيرة حدود T الدنيا على F هي المضاعف المشترك الأصغر لكثيرات الحدود $q_1(x),..,q_k(x)$.

إن برهان هذه النتيجة متروك للقارىء.

ليكن $T\in A_F(V)$ ولنفرض أن كثيرة حدود T الدنيا على F هي $p(x)\in F[x]$ ، عندئذ استنادا إلى تمهيدية (٣-٩-٥) نستطيع أن نفرق $p(x)\in F[x]$ بطريقة وحيدة على الشكل $p(x)=q_1(x)^{l_1}q_2(x)^{l_2}...q_k(x)^{l_k}$ ، حيث $q_i(x)$ كثيرة حدود غير مختزلة في $F[x]$ ، كما أن $l_1,l_2,...,l_k$ أعداد صحيحة موجبة. إن هدفنا هو تفريق V على هيئة مجموع مباشر لفضاءات جزئية غير متغيرة تحت تأثير T بحيث يكون لكل تحويل خطي من التحويلات الخطية المحدثة بواسطة T كثيرة حدود دنيا هي قوة لكثيرة حدود غير مختزلة. إذا كان $k=1$ فإن V يحقق ما نتطلبه ولذلك نفرض أن $k>1$.

ليكن :

$V_1=\{v\in V|vq_1(T)^{l_1}=0\}$ و $V_2=\{v\in V|vq_2(T)^{l_2}=0\},...,\ V_k=\{v\in V|vq_k(T)^{l_k}=0\}$.

إن من الواضح أن V_i فضاء جزئي من V ، لكل i ، وبالإضافة إلى ذلك، فإن V_i غير متغير تحت تأثير T ، لأنه إذا كان $u\in V_i$، وبما أن T يتبادل مع $q_i(T)$، فإننا نجد أن :

$$(uT)q_i(T)^{l_i}=(uq_i(T)^{l_i})T=0T=0$$

ومن تعريف V_i نجد أن $uT\in V_i$. ليكن T_i هو التحويل الخطي المحدث بواسطة T على V_i.

مبرهنة (٦-٦-١)

$V_i \neq (0)$ لكـل i ، $i=1,2,\ldots,k$ ، أيضـا $V=V_1 \oplus \ldots \oplus V_k$. كما أن كثيرة حدود T_i الدنيا هي $q_i(x)^{l_i}$.

البرهان

إذا كان $k=1$ فإن $V=V_1$ ، ومن ثم فإنه لا يوجد شيء يستدعى البرهان. لذلك نفرض أن $k>1$.

نريد أن نثبـت أولا أن $V_i \neq (0)$ ، ولإنجـاز هذا نقـدم كثـيرات الحـدود الـتي عددها k:

$$h_1(x)=q_2(x)^{l_2}q_3(x)^{l_3}\ldots q_k(x)^{l_k}$$

$$h_2(x)=q_1(x)^{l_1}q_3(x)^{l_3}\ldots q_k(x)^{l_k}$$

$$h_i(x)=\prod_{j\neq 1} q_j(x)^{l_j},\ldots,$$

$$\vdots$$

$$h_k(x)=q_1(x)^{l_1}q_2(x)^{l_2}\ldots q_{k-1}(x)^{l_{k-1}}$$

بما أن $k>1$ و $h_i(x)\neq p(x)$ ، لذلك فإن $h_i(T)\neq 0$. عليه فإنه لكل i ، يوجد $v\in V$ بحيث أن $w=vh_i(T)\neq 0$ ، بيد أنه عندئذ

$$wq_i(T)^{l_i}=v(h_i(T)q_i(T)^{l_i})=vp(T)=0$$

وبالتالي فإن $0\neq w_i \in V_i$ ومن ثم فإن $V_i\neq(0)$. في الحقيقية لقد أثبتنا أكثر من ذلك وهو أن $0\neq V_{h_i}(T)\subset V_i$. هنـاك ملاحـظة أخـرى في هذا السياق حول $h_i(x)$ هي أنه إذا كان $v_j \in V_j$ حيث $j\neq i$ ولما كان $q_j(x)^{l_j}|h_i(x)$ ، لذا فإن $v_jh_i(T)=0$.

إن كثـيرات الحـدود $h_1(x),h_2(x),\ldots,h_k(x)$ أولية نسبيا (أثبت ذلك) وبالتالي فإنه استنادا إلى تمهيدية (٣-٩-٤) يكون بإمكاننا إيجاد كثيرات حدود $\alpha_1(x),\ldots,\alpha_k(x)\in F[x]$ بحيث يكون $\alpha_1(x)h_1(x)+\ldots+\alpha_k(x)h_k(x)=1$ ومن هنا نجد أن

$$\alpha_1(T)h_1(T)+\ldots+\alpha_k(T)h_k(T)=1.$$

ومن ثم، إذا كان $v\in V$ فإن :

$$v=v1=v(\alpha_1(T)h_1(T)+\ldots+\alpha_k(T)h_k(T))=v\alpha_1(T)h_1(T)+\ldots+v\alpha_k(T)h_k(T)$$

الأن $v\alpha_i(T)h_i(T)\in Vh_i(T)$ لكل i ، ولما كنا قد أثبتنا أعلاه أن $Vh_i(T)\subset V_i$ لذا فإننا قد كتبنا v على الصيغة $v=v_1+\ldots+v_k$ ، حيث ، $v_i=v\alpha_i(T)h_i(T)\in V_i$ وبعبارة أخرى فإن

$$V=V_1+\ldots+V_k$$

يجب علينا، الآن، أن نتحقق من أن هذا الجمع هو جمع مباشر، ولإيضاح ذلك يكفي أن نثبت أنه إذا كان $u_1+\ldots+u_k=0$ حيث $u_i\in V_i$ فإن $u_i=0$ لكل i. لهذا نفرض أن $u_1+\ldots+u_k=0$ وأن $u_i=0$ ، لبعض قيم i. بضرب هذه العلاقة بـ $h_1(T)$ نحصل على :

$$u_1h_1(T)+\ldots+u_kh_1(T)=0h_1(T)=0$$

ومع ذلك فإن $u_jh_1(T)=0$ ، $j\neq1$ ولما كان $u_j\in V_j$ لذا فإن المعادلة تتقلص إلى $u_1h_1(T)=0$ ، ولكن عندئذ $u_1q_1(T)^{l_1}=0$. وبما أن $h_i(x)$ و $q_i(x)$ أوليتان نسبيا فإن هذا يقتضي أن $u_1=0$ (أثبت ذلك) الأمر الذي لا يتفق مع افتراض أن $u_1\neq0$. وهكذا نكون قد برهنا على أن :

$$V=V_1\oplus\ldots\oplus V_k$$

لإتمام البرهان، يجب علينا إثبات أن كثيرة حدود T_i الدنيا المعرف على V_i هي $q_i(x)^{l_i}$.

من تعريف V_i وبما أن $V_iq_i(T)^{l_i}=0$ ، لذلك فإن $q_i(T_i)^{l_i}=0$ ولهذا فإن معادلة T_i الدنيا يجب أن تكون قاسما لـ $q_i(x)^{l_i}$ ، أي من الصيغة $q_i(x)^{f_i}$ ، $f_i\leq l_i$.

ومن نتيجة التمهيدية (٦-٦-١) فإن كثيرة حدود T الدنيا على F هي المضاعف المشترك الأصغر لـ $q_k(x)^{f_k},\ldots,q_1(x)^{f_1}$ ، أي يجب أن يكون $q_1(x)^{f_1}\ldots q_k(x)^{f_k}$ ولما كانت كثيرة الحدود الدنيا هذه هي في الحقيقة $q_1(x)^{l_1}\ldots q_k(x)^{l_k}$ ، لذلك فإن $f_1\geq l_1,f_2\geq l_2,\ldots,f_k\geq l_k$. وبمقارنة هذه مع المتباينة الواردة أعلاه نحصل على $l_i=f_i$ لكل i ، $i=1,2,\ldots,k$. وبهذا يتم إثبات المبرهنة.

إذا حدث وكانت جميع الجذور المميزة لـ T تنتمي إلى F فإن كثيرة الحدود الدنيا لـ T تأخذ صيغة أفضل هي $q(x)=(x-\lambda_1)^{l_1}\ldots(x-\lambda_k)^{l_k}$ حيث $\lambda_1,\ldots,\lambda_k$ هي الجذور المميزة المختلفة لـ T. إن العوامل الغير مختزلة $q_i(x)$ الواردة أعلاه هي $q_i(x)=x-\lambda_i$. لاحظ هنا أن للتحويل الخطي T_i على V_i جذرًا مميزًا واحدًا هو λ_i فقط.

نتيجة

إذا كانت جميع جذور T المميزة المختلفة $\lambda_1,\ldots,\lambda_k$ تنتمي إلى F فإنه يمكن كتابة V على الصيغة $V=V_1\oplus\ldots\oplus V_k$ حيث $V_i=\{v\in V|v(T-\lambda_i)^{l_i}=0\}$ كما أن التحويل T_i على V_i له جذر مميز واحد فقط هو λ_i.

الآن نعود قليلا إلى المبرهنة، سنستخدم الاصطلاحات نفسها الواردة في المبرهنة مثل T_i ، V_i. لما كان $V=V_1\oplus\ldots\oplus V_k$ وإذا كان $\dim V_i=n_i$ فإنه وفقا لتمهيدية (٦-٥-١) نستطيع إيجاد أساس لـ V بحيث تأخذ مصفوفة T بالنسبة لهذا الأساس الصيغة

$$\begin{pmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & A_k \end{pmatrix}$$

حيث كل من A_i مصفوفة من النوع $n_i\times n_i$ والتي هي في الواقع مصفوفة T_i.

ولكن ما الذي نبحث عنه بالضبط؟ إننا نريد عنصرا في فصل تشابه T الذي نستطيع تمييزه بطريقة ما. يمكن صياغة هذا على ضوء المبرهنة (٦-٣-٢) وذلك كما يلي: إننا نبحث عن أساس لـ V لكي تأخذ مصفوفة T صيغة بسيطة بالنسبة لهذا الأساس. استناداً إلى المناقشة الواردة آنفا فإنه يمكن حصر هذا البحث عن التحول الخطي T_i. من هنا يمكن اختصار المسألة العامة من مناقشة تحويلات خطية عامة إلى تحويلات خطية خاصة تكون كثيرات حدودها الدنيا قوى لكثيرات حدود غير مختزلة. وسنناقش بعد قليل الحالة الخاصة التي تنتمي فيها جذور T المميزة إلىF . سنناقش في البند القادم الحالة العامة والتي لن نضع فيها أية قيود على الجذور المميزة لـ T.

نحن الآن في وضع أفضل، ذلك أن جميع المعلومات متوفرة لدينا وما علينا سوى أن نضعها في قالب واحد. إن هذا يؤدي إلى المبرهنة المهمة والمفيدة والتي فيها نعرض لما يدعى **بصيغة جوران القانونية** (Jordan canonical form) وقبل أن نعرض المبرهنة نعطي التعريف الآتي.

تعريف

إن المصفوفة

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & & \dots & . \\ . & & & & . \\ . & & & & . \\ . & & & & 1 \\ 0 & . & . & \dots & \lambda \end{pmatrix}$$

حيث الأعداد λ في القطر الرئيس والأعداد 1 في القطر فوق الرئيس وأصفار فيما سوى ذلك ، تدعى قالب جوردان الأساسي الذي يتبع λ.

مبرهنة (٦-٦-٢)

لتكن جميع جذور $T \in A_F(V)$ المميزة المختلفة $\lambda_1,\dots,\lambda_k$ تنتمي إلى F. عندئذ يمكن إيجاد أساس لـ V بحيث تكون مصفوفة T بالنسبة لهذا الأساس على الهيئة

$$\begin{pmatrix} J_1 & & & & \\ & J_2 & & & \\ & & \ddots & & \\ & & & & J_k \end{pmatrix}$$

حيث

$$J_i = \begin{pmatrix} B_{i_1} & & & & \\ & B_{i_2} & & & \\ & & \ddots & & \\ & & & & B_{ir_i} \end{pmatrix}$$

كما أن $B_{i_1},..,B_{ir_i}$ هي قوالب جوردان الأساسية التي تتبع λ_i.

البرهان

أولا ، وقبل أن نبدأ، إن قالب جوردان الأساسي من النوع $m \times m$ الذي يتبع λ هو $\lambda + M_m$ حيث M_m هي المصفوفة المعرفة بعد برهان تمهيدية (٦-٥-٢) .

من تمهيدية (٦ـ٥ـ١) ونتيجة مبرهنة (٦ـ٦ـ١) يمكن أن نختصر الوضع إلى الحالة التي يكون فيها جذر مميز واحد لـ T ، أي عندما يكون T−λ معدوم القوى. وهكذا فإن T=λ+(T−λ) وحيث إن T−λ معدوم القوى لذا فإنه وفقا لمبرهنة (٦ـ٥ـ١) يوجد أساس بحيث تأخذ مصفوفة T−λ بالنسبة إليه الصيغة:

$$\begin{pmatrix} M_{n_1} & & \\ & \ddots & \\ & & M_{n_r} \end{pmatrix}$$

وعندئذ تأخذ مصفوفة T الصيغة

$$\begin{pmatrix} M_{n_1} & & \\ & \ddots & \\ & & M_{n_r} \end{pmatrix} + \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{pmatrix} = \begin{pmatrix} B_{n_1} & & \\ & \ddots & \\ & & B_{n_r} \end{pmatrix}$$

حيث إننا استخدمنا الملاحظة الواردة في أول البرهان حول العلاقة بين قوالب جوردان الأساسية والمصفوفات M_m وبهذا ينتهي البرهان.

باستخدام مبرهنة (٦ـ٥ـ١) نستطيع ترتيب الأمور بحيث يكون سعة $B_{i_1} \leqslant$ سعة $B_{i_2} \leqslant$... وذلك في كل J_i. وعندما يتم عمل هذا فإن المصفوفة

$$\begin{pmatrix} J_k & & \\ & \ddots & \\ & & J_k \end{pmatrix}$$

تسمى *صيغة جوردان للتحويل T*. لاحظ أن مبرهنة (٦ـ٦ـ٢) في حالة المصفوفات معدومة القوى تختزل إلى مبرهنة (٦ـ٥ـ١).

نترك برهان العبارة التالية كتمرين: *يكون التحويلان الخطيان في $A_F(V)$ والتي تنتمي جذورهما المميزة إلى F متشابهين إذا وفقط إذا أمكن تحويلهما إلى صيغة جوردان واحدة.*

وهكذا فإن صيغة جوردان تعمل، كمعيِّن، لفصول التشابه لهذا النوع من التحويلات الخطية.

ويمكن إعادة صياغة المبرهنة (٦-٦-٢) بدلالة المصفوفات وذلك كما يلي : *لتكن $A \in F_n$ ولنفرض أن K هو حقل انشطار كثيرة الحدود الدنيا لـ A على F* ، *عندئذ يمكن إيجاد مصفوفة $C \in K_n$ لها معكوس بحيث تأخذ المصفوفة CAC^{-1} صيغة جوردان .*

سنترك بعض الأمور البسيطة والمتعلقة بالانتقال من مبرهنة (٦-٦-٢) إلى الصيغة المصفوفية، المعطاة آنفا، للقارىء

ملاحظة

إذا كانت $A \in F_n$ وإذا كان في K_n ، حيث K هو حقل انشطار كثيرة الحدود الدنيا لـ A على F ،

$$CAC^{-1} = \begin{pmatrix} J_1 & & & & \\ & J_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & J_k \end{pmatrix}$$

حيث يقابل كل J_i جذرًا مميزًا مختلفًا λ_i للمصفوفة A فإن **تكرار** (multiplicity) λ_i باعتباره جذرًا مميزًا لـ A ، يعرف بأنه n_i ، حيث J_i هي المصفوفة من النوع $n_i \times n_i$. لاحظ هنا أن مجموع التكرارات يساوي n .

ومن الواضح أنه يمكن أن نعرف تكرار الجذر المميز للتحويل الخطي بصورة مشابهة لما قدم أعلاه .

مسائل

١ - إذا كان S و T تحويلين خطيين معدومي القوى وكان ST=TS. فأثبت أن ST و S+T هما تحويلان خطيان معدوما القوى .

٢ - أثبت باستخدام حسابات مصفوفية مباشرة أن المصفوفتين

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ و } \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

غير متشابهتين .

٣ - إذا كان $n_1 \geqslant n_2$ و $m_1 \geqslant m_2$. فأثبت باستخدام حسابات مصفوفية مباشرة أن

$$\begin{pmatrix} M_{m_1} & \\ & M_{m_2} \end{pmatrix} \quad و \quad \begin{pmatrix} M_{n_1} & \\ & M_{n_2} \end{pmatrix}$$

متشابهتان إذا وفقط إذا كان $n_1=m_1$ و $n_2=m_2$.

٤* - إذا كان $n_1 \geqslant n_2 \geqslant n_3$ و $m_1 \geqslant m_2 \geqslant m_3$ ، فأثبت باستخدام حسابات مصفوفية مباشرة أن:

$$\begin{pmatrix} M_{m_1} & & \\ & M_{m_2} & \\ & & M_{m_3} \end{pmatrix} \quad و \quad \begin{pmatrix} M_{n_1} & & \\ & M_{n_2} & \\ & & M_{n_3} \end{pmatrix}$$

متشابهتان إذا وفقط إذا كان $n_1=m_1$ و $n_2=m_2$ و $n_3=m_3$

٥ - (ا) أثبت أن المصفوفة:

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

معدومة القوى ثم أوجد لا متغيراتها وصيغة جوردان لها.

(ب) أثبت أن المصفوفة في الفقرة (ا) ليست مشابهة للمصفوفة

$$\begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix}$$

٦ - برهن على تمهيدية (٦-٦-١) ونتيجتها حتى ولو كان الجمع الوارد فيها ليس جمعا مباشرًا.

٧ - برهن على العبارة الآتية: يكون التحويلان الخطيان في $A_F(V)$ واللذان تنتمي جميع جذورهما المميزة إلى F متشابهين إذا وفقط إذا كان لهما صيغة جوردان نفسها (بغض النظر عن ترتيب الجذور المميزة).

٨ - أثبت الصيغة المصفوفية لمبرهنة (٦-٦-٢) والواردة قبل هذه المسائل.

٩ - برهن على أن المصفوفة من النوع $n \times n$.

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \cdot & & \cdot & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot & \cdot \\ \cdot & & & & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

حيث العدد 1 في القطر تحت الرئيس وصفر فيما سوى ذلك، متشابهة مع المصفوفة M_n.

١٠ - إذا كان مميز F هو $p>0$. فأثبت أن المصفوفة $A=\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ تحقق $A^p=1$.

١١ - إذا كان مميز F يساوي صفرًا. فأثبت أن المصفوفة $A=\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ تحقق $A^m=1$ فقط عندما $\alpha=0$ ، حيث $m>0$.

١٢ - أوجد جميع صيغ جوران الممكنة لما يلي:

(ا) جميع المصفوفات من النوع 8×8 التي كثيرة حدودها الدنيا هي $x^2(x-1)^3$.

(ب) جميع المصفوفات من النوع 10×10 على حقل مميزه لا يساوي 2 والتي كثيرة حدودها الدنيا هي $x^2(x-1)^2(x+1)^3$.

١٣ - أثبت أن المصفوفة A من النوع $n\times n$ ، حيث

$$A=\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \cdot & & \cdot & \cdot & \cdot \\ \cdot & & & \cdot & \cdot \\ \cdot & & & & \cdot \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

تشابه المصفوفة

$$\begin{pmatrix} n & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \cdot & & \cdot & \cdot & \cdot \\ \cdot & & & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

وذلك إذا كان مميز F يساوي صفرًا أو يساوي p حيث $p \nmid n$. وما هو تكرار الصفر كجذر مميز لـ A ؟

يقال عن المصفوفة $A=(a_{ij})$ إنها مصفوفة *قطرية* إذا كان $a_{ij}=0$ لكل $i\neq j$ ، أي إذا كانت العناصر خارج القطر الرئيس أصفارًا. ويقال عن المصفوفة (أو التحويل الخطي) إنه **قابل للاستقطار** (diagonalizable) وذلك إذا كانت مشابهة لمصفوفة قطرية (وبالنسبة للتحويل الخطي يوجد له مصفوفة بالنسبة لأساس معين بحيث تكون هذه المصفوفة قطرية).

١٤ - إذا كان $T\in A(V)$ فإنه يكون قابلا للاستقطار (إذا كانت جميع جذوره المميزة تنتمي إلى F) إذا وفقط إذا كان $v(T-\lambda)^m=0$ حيث $v\in V$ و $\lambda\in F$ فإن $v(T-\lambda)=0$.

١٥ - أثبت باستخدام المسألة (١٤) أنه إذا كان $E^2=E$ فإن E قابل للاستقطار.

١٦ - إذا كان $E^2=E$ و $F^2=F$ فإن E و F متشابهان إذا وفقط إذا كان لهما المرتبة نفسها.

١٧ - إذا كان تكرار كل جذر مميز لـ T يساوي 2 وكانت جميع الجذور المميزة لـ T تنتمي إلى F ، فأثبت أنه يمكن استقطار T.

١٨ - إذا كان مميز F يساوي صفرًا وكان $T\in A_F(V)$ يحقق $T^m=1$ فأثبت أنه إذا كانت الجذور المميزة لـ T تنتمي إلى F فإن T قابل للاستقطار (*إرشاد:* استخدم صيغة جوردان لـ T).

*١٩- إذا كانت $A,B\in F_n$ قابلتين للاستقطار وكان $AB=BA$. فأثبت أنه يوجد عنصر $C\in F_n$ بحيث أن كلا من CAC^{-1} و CBC^{-1} قطرية.

٢٠ - أثبت أن نتيجة المسألة (١٩) غير صحيحة وذلك في حالة كون $AB\neq BA$.

(٦-٧) الصيغ القانونية: الصيغة القانونية النسبية

إن صيغة جوردان هي الأكثر استعمالا لإثبات مبرهنات حول التحويلات الخطية والمصفوفات. ولسوء الحظ، هناك عقبة معضلة هي أنها تضع شروطا على موقع الجذور المميزة. صحيح أنه إذا كانت جذور $T\in A_F(V)$ (أو $A\in F_n$) المميزة ليست في F فإننا نضطر إلى استخدام الامتداد المنتهي K لـ F بحيث يحوي K على جميع الجذور المميزة لـ T وبعد ذلك نحول T إلى صيغة جوردان على K. إن هذا، في الواقع، إجراء قياسي ومع ذلك فإنه يبرهن النتيجة في K_n وليس في F_n. ولكنه يوجد مناسبات عديدة

تكـون فيهـا النتيجـة مبرهنـة من أجـل $A \in F_n$ باعتبـارهـا عنصراً في K_n ولا يمكن الرجوع من K_n لنحصل على المعلومات المطلوبة في F_n.

لهذا فإننا نحتاج إلى صيغة قانونية لعناصر في $A_F(V)$ (أو F_n) التي لا نفـترض أي شيء حول موقع الجذور المميزة لهذه العناصر، أي نحتاج إلى صيغة قانونية ومجموعة من غير المتغيرات في $A_F(V)$ نفسها، مستخدمين فقط عناصرها وعملياتها. إن هذه الصيغة القانونية تتمثل لنا بما يسمى **الصيغة القانونية النسبية** (Rational canonical form) والتي سترد في المبرهنة (٦-٧-١) ونتيجتها.

ليكن $T \in A_F(V)$. إننـا نقـترح أن نجعـل من V فضاءً حلقيًا على $F[x]$ حيث $F[x]$ هي حلقة كثيرات الحدود في x على F وذلك باستخدام T. ونبدأ ذلك بتعريف لأي كثيرة حدود $f(x)$ في $F[x]$ وأي قيمة $v \in V$ يكون $f(x)v = vf(T)$. ونترك للقارىء التحقق من أنه بهذا التعريف، أي بضرب عناصر V بعناصر $F(x)$، يصبح V فضاءً حلقيًا على $F(x)$.

وحيث إن V منتهي البعد على F لذلك فإنه يكون منتهي التوليد على F وهذا بدوره يجعله منتهي التوليد على $F[x]$ التي تحوي F. (وفضلا عن ذلك فإن $F[x]$ حلقية إقليدية وباعتبار V فضاءً منتهي التوليد على $F[x]$ فإنه وفقا لمبرهنة (٤-٥-١) يكون V مجموعًا مباشرا لعدد منته من الفضاءات الجزئية الحلقية الدورية. واستنادا إلى الطريقة التي قدمنا بها بناء الفضاء الحلقي على F، فإن كل واحد من هذه الفضاءات الجزئية الحلقية غير متغير تحت تأثير T. وبالإضافة إلى ذلك فإنه يوجد عنصر m_0 في الفضاء الجزئي الحلقي M بحيث يكون كل عنصر $m \in M$ من الصيغة $m = m_0 f(T)$، حيث $f(x) \in F[x]$.

لكي نعين طبيعة تأثير T على V فإنه، من أجل ذلك، يكفي أن نعرف تأثير T على الفضاء الجزئي الحلقي، وهذا هو ما نريد تعيينه تماما.

أولا: نفرق V مبدئيا، كما فعلنا في مبرهنة (٦-٦-١)، وذلك وفق تفريق كثيرة حدود T الدنيا إلى حاصل ضرب كثيرات حدود غير مختزلة.

لنفـرض أن كثـيرة حدود T الـدنيا على F هي $p(x) = q_1(x)^{e_1} \ldots q_k(x)^{e_k}$ حيث $q_i(x)$ كثيرات حدود غير مختزلة في $F[x]$ كما أن $e_i > 0$ لكل i. عندئذ وكما رأينا في مبرهنة (٦-٦-١):

$$V=V_1\oplus\ldots\oplus V_k$$

حيث كل من V_i غير متغير بالنسبة لـ T ، كما أن $q_i(x)^{e_i}$ هي كثيرة حدود T الدنيا على V_i. ولمعرفة طبيعة الفضاء الجزئي الحلقي، من أجل تحويل خطي T فإننا نرى، من هذه المناقشة، أنه يكفي أن نعلم طبيعة T الذي كثيرة حدوده الدنيا هي قوة لكثيرة حدود غير مختزلة.

نبدأ ببرهان التمهيدية الآتية.

تمهيدية (٦-٧-١)

لنفرض أن كثيرة حدود $T\in A_F(V)$ الدنيا على F هي $p(x)=\gamma_0+\gamma_1x+\ldots+\gamma_{r-1}x^{r-1}+x^r$. ولنفرض أن V باعتباره فضاءً حلقيًا (كما هو موصوف أعلاه) هو فضاء حلقي دوري (أي دوري بالنسبة لـ T). عندئذ يوجد أساس لـ V على F بحيث تكون مصفوفة T بالنسبة لهذا الأساس هي

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\gamma_0 & -\gamma_1 & \cdot & \cdots & -\gamma_{r-1} \end{pmatrix}$$

البرهان

لما كان V دوريًا بالنسبة لـ T فإنه يوجد متجه $v\in V$ بحيث يكون كل عنصر $w\in V$ من الصيغة $w=vf(T)$ حيث $f(x)\in F[x]$.

فإذا حدث وأن حقق كثيرة حدود $s(x)$ حيث $s(x)\in F[x]$ العلاقة $vs(T)=0$. فإنه لأي $w\in V$ يكون

$$ws(T)=(vf(T)s(T))=vs(T)f(T)=0$$

وهكذا فإن $s(T)$ يفني جميع عناصر T، لذلك فإن $s(T)=0$. وعندئذ $p(x)|s(x)$ لأن $p(x)$ هي كثيرة حدود T الدنيا. إن هذه الملاحظة تقتضي أن $v,vT,\ldots,vT^{r-1}$ مستقلة خطيًا على F لأنه لو كان الأمر خلاف ذلك فإن

$$a_0v+a_1vT+\ldots+a_{r-1}vT^{r-1}=0$$

حيث $a_0,a_1,\ldots,a_{r-1}\in F$. وعندئذ فإن

$$v(a_0+a_1T+\ldots+a_{r-1}T^{r-1})=0$$

واستنادا إلى المناقشة الواردة أعلاه يكون :

$$p(x)|(a_0+a_1x+\ldots+a_{r-1}x^{r-1})$$

ومن الواضح أن هذا غير ممكن إذ أن درجة $p(x)$ هي r ما لم يكن $a_0=a_1=..=a_{r-1}=0$. وحيث إن

$$T^r=-\gamma_0-\gamma_1T-\ldots-\gamma_{r-1}T^{r-1}$$

فإنه يكون لدينا T^{r+k} حيث $k\geq 0$ تركيب خطي لـ $1,T,\ldots,T^{r-1}$ على F ، وكذلك فإن $f(T)$ ، لأي $f(x)\in F[x]$ ، هو تركيب خطي لـ $1,T,\ldots,T^{r-1}$ على F ولما كان أي $w\in V$ هو من الصيغة $w=vf(T)$. لذا فإننا نجد أن w تركيب خطي لـ $v,vT,\ldots,vT^{r-1}$.

لقد برهنا أعلاه على أن العناصر $v,vT,\ldots,vT^{r-1}$ هي أساس لـ V على F. ويمكن التحقق مباشرة من أن مصفوفة T بالنسبة لهذا الأساس هي المصفوفة الواردة في التمهيدية .

تعريف

إذا كان $f(x)\in F[x]$ ، حيث $f(x)=\gamma_0+\gamma_1x+\ldots+\gamma_{r-1}x^{r-1}+x^r$ فإن المصفوفة

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & & . & . & . \\ . & & & . \quad . & . \\ . & & & \quad . & . \\ 0 & 0 & 0 & \ldots & 1 \\ -\gamma_0 & -\gamma_1 & . & \ldots & -\gamma_{r-1} \end{pmatrix}$$

*من النوع $r\times r$ تدعى **بالمصفوفة المصاحبة** (Companion matrix) لـ $f(x)$ وسنكتبها على الشكل $C(f(x))$.*

لاحظ أن تمهيدية (٦-٧-١) تنص على أنه

إذا كان V دوريا بالنسبة لـ T وكانت كثيرة حدود T الدنيا في $F[x]$ هي $p(x)$ فإن مصفوفة T بالنسبة لأساس ما لـ V هي $C\left(p(x)\right)$.

لاحظ كذلك أن المصفوفة $C(p(x))$ ، حيث $f(x)$ هي أي كثيرة حدود واحدية في $F[x]$ ، تحقق $f(x)$ ، كما أن كثيرة حدودها الدنيا هي $f(x)$ (انظر مسألة (٤) الواردة في نهاية هذا البند ومسألة (٢٩) الواردة في نهاية البند (٦-١).

الآن نأتي إلى إثبات المبرهنة المهمة الآتية.

مبرهنة (٦-٧-١)

إذا كانت كثيرة حدود T الدنيا، حيث $T\in A_F(V)$ ، هي $p(x)=q(x)^e$ ، بحيث $q(x)$ كثيرة حدود واحدية غير مختزلة في $F[x]$ ، فإنه يمكن إيجاد أساس لـ V على F بحيث تكون مصفوفة T من الصيغة

$$\begin{pmatrix} C(q(x)^{e_1}) & & & \\ & C(q(x)^{e_2}) & & \\ & & \ddots & \\ & & & C(q(x)^{e_r}) \end{pmatrix}$$

حيث $e=e_1\geqslant e_2\geqslant\ldots\geqslant e_r$.

البرهان

لما كان V ، باعتباره فضاءً حلقيًّامنتهيالتوليد على $F[x]$ ، ولما كانت $F[x]$ حلقة إقليدية فإننا نستطيع تفريق V على الصيغة $V=V_1\oplus\ldots\oplus V_r$، حيث إن V_i فضاء حلقي دوري وغير متغير تحت تأثير T. فإذا كان T_i هو التحويل الخطي المحدث بواسطة T على V_i ، فإن كثيرة حدوده الدنيا يجب أن تكون قاسما لـ $p(x)=q(x)^e$. وبالتالي فهو من الصيغة $q(x)^{e_i}$ وباستطاعتنا ترقيم الفضاءات بحيث يكون $e_1\geqslant e_2\geqslant\ldots\geqslant e_r$.

الآن $q(T)^{e_1}$ يفني V_i لكل i وبالتالي فهو يفني V ومن ثم فإن $q(T)^{e_1}=0$. وهكذا فإن $e_1\geqslant e$ ولما كان من الواضح أن e_1 هو على الأكثر e لذا نجد أن $e_1=e$.

استنادا إلى تمهيدية (٦ـ٧ـ١) وحيث إن V_i دوري بالنسبة إلى T ، فإننا نستطيع إيجاد أساس بحيث تكون مصفوفة التحويل الخطي T_i على V_i هي $C(q(T))^{e_i}$. وهكذا واستنادا إلى مبرهنة (٦ـ٦ـ١) يمكن إيجاد أساس لـ V بحيث تكون مصفوفة T بالنسبة لهذا الأساس هي

$$\begin{pmatrix} C(q(x)^{e_1}) & & & & \\ & C(q(x)^{e_2}) & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad C(q(x)^{e_r}) \end{pmatrix}$$

نتيجة

إذا كانت كثيرة حدود $T\in A_F(V)$ الدنيا على F هي $p(x)=q_1(x)^{l_1}\ldots q_k(x)^{l_k}$ حيث $q_1(x),\ldots,q_k(x)$ كثيرات حدود مختلفة وغير مختزلة في $F[x]$ فإنه يمكن إيجاد أساس لـ V بحيث تكون مصفوفة T من الصيغة

$$\begin{pmatrix} R_1 & & & & \\ & R_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad R_k \end{pmatrix}$$

حيث كل من

$$R_i = \begin{pmatrix} C(q_i(x)^{e_{i1}}) & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \quad C(q_i(x)^{e_{ir_i}}) \end{pmatrix}$$

كما أن $e_i=e_{i1}\geqslant e_{i2}\ldots\geqslant e_{ir_i}$

البرهان

استنادًا إلى مبرهنة (٦ـ٥ـ١) يمكن تفريق V إلى حاصل الجمع المباشر $V=V_1\oplus\ldots\oplus V_k$ ، حيث كل من V_i غير متغير تحت تأثير T. كما أن كثيرة الحدود الدنيا للتحويل الخطي T_i المحدث بواسطة T على V_i هي $q_i(x)^{e_i}$. وباستخدام تمهيدية

(٦ـ٥ـ١) المبرهنة آنفا نحصل على المطلوب . فإذا كانت درجة $q_i(x)$ هي d_i فإننا نلاحظ أن $\sum_i d_i e_{ij}=n$ حيث n هو بعد V على F.

تعريف

*إن مصفوفة T الواردة في النتيجة الآنفة الذكر تدعى **بالصيغة القانونية النسبية** لـ T.*

تعريف

يطلق على كثيرات الحدود

$$q_1(x)^{e_{11}}, q_1(x)^{e_{12}}, \ldots, q_1(x)^{e_{1r_1}}, \ldots, q_k(x)^{e_{k1}}, \ldots, q_k(x)^{e_{kr_k}}$$

*في F[x] **القواسم الابتدائية** لـ T.*

تعريف

*إذا كان $dim_F V=n$ فإن **كثيرة الحدود المميزة لـ T** ونرمز لها بـ $p_T(x)$ هي حاصل ضرب قواسمه الابتدائية .*

سنطابق بين كثيرة الحدود المميزة المعرفة آنفا وكثيرة حدود أخرى سنكوِّنها في البند (٦ـ٩) . إن كثيرة حدود T المميزة هي كثيرة حدود من الدرجة n وتنتمي إلى F[x] ، كما أن لها خواص مهمة إحداها هي الواردة في الملاحظة الآتية .

ملاحظة

كل تحويل خطي $T \in A_F(V)$ يحقق كثيرة حدوده المميزة ، كما أن كل جذر مميز لـ T هو جذر لـ $p_T(x)$.

ملحوظة (١)

إن العبارة الأولى من هذه الملاحظة هي نص مبرهنة مشهورة وهي مبرهنة كيلي ـ هاملتون ومع ذلك فإن تسميتها بالصيغة التي أوردناها ليس عدلاً . إن فحوى مبرهنة

كيلي ـ هاملتون هي في الحقيقة أن T تحقق $p_T(x)$ عندما تعطى $p_T(x)$ بصيغة محددة جدًّا وإذا أمكن تكوينها بسهولة من T. ومع ذلك فإن الملاحظة بصيغتها الواردة تحوي على شيء ذي قيمة. ذلك أنه لما كانت كثيرة الحدود المميزة هي كثيرة حدود من الدرجة n فإننا قد أثبتنا أن كل عنصر في $A_F(V)$ يحقق بالفعل كثيرة حدود من درجة n واقعة في F[x]. وحتى الآن، لقد برهـنا هنا الحالة للتحويلات الخطيـة التي تقع جذورها المميـزة في F.

ملحوظة (٢)

إن العبارة الثانية من الملاحظة كما وردت لا تحوي أي شيء، لأنه متى ما كان T يحقق كثيرة حدود فإن كل جذر مميز لـ T يحقق كثيرة الحدود هذه وبالتالي فإنه لن يكون لـ $p_T(x)$ أي خصوصية إذا كان ما ورد في المبرهنة صحيحا بالنسبة لها. بيد أن الواقع هو كما يلي: كل جذر مميز لـ T هو جذر مميز لـ $p_T(x)$، وبالعكس فإن أي جذر لـ $p_T(x)$ هو جذر مميز لـ T. وفضلا عن ذلك فإن تكرار أي جذر لـ $p_T(x)$ باعتباره جذرا لكثيرة الحدود يساوي تكراره باعتباره جذرا مميزا لـ T. وباستطاعتنا برهان ذلك الآن، لكننا سنؤجله إلى وقت لاحق وذلك عندما نستطيع برهانه بصورة طبيعية أكثر.

برهان الملاحظة

يجب إثبات أن T تحقق $p_T(x)$، ولكن هذا بسيط إلى حد كبير، ذلك أنه بما أن $p_T(x)$ هى حاصل ضرب

$$q_1(x)^{e11},q_1(x)^{e12},\ldots,q_k(x)^{ek1},\ldots,\ldots$$

وبما أن:

$$e_{11}=e_1,\ e_{21}=e_2,\ \ldots,\ e_{k1}=e_k$$

لهذا فإن $p_T(x)$ تقبل القسمة على

$$p(x)=q_1(x)^{e1}\ldots q_k(x)^{ek}$$

والتي هي كثيرة حدود T الدنيا. ولما كان $p(T)=0$ لذا فإن $p_T(T)=0$.

لقد أطلقنا على مجموعة كثيرات الحدود الواردة في الصيغة القانونية النسبية لـ T القـواسم الابتـدائية لـ T. إنـه لمرغوب إلى درجة كبيرة توضيح ما إذا كانت القواسم

الابتدائية تعني التشابه في $A_F(V)$ إذ أن فصول التشابه، عندئذ، ستكون في تقابل مع مجموعة كثيرات الحدود في $F[x]$. ولكن قبل أن نثبت هذا فإننا سنثبت النتيجة التي تقتضي أن يكون لتحويلين خطيين القواسم الابتدائية نفسها.

مبرهنة (٦-٧-٢)

ليكن V و W فضائي متجهات على F وليكن ψ هو تماثل فضاء متجهات من V على W. ولنفرض أن $S\in A_F(V)$ و $T\in A_F(W)$ بحيث أن $(vS)\psi=(v\psi)T$ لكل $v\in V$ عندئذ يكون لـ S و T القواسم الابتدائية نفسها.

البرهان

إذا كان $v\in V$ فإن

$$(vS^2)\psi=((vS)S)\psi=((vS)\psi)T=((v\psi)T)T=v\psi T^2$$

ومن الواضح أنه بالاستمرار على هذا النحو فإننا نجد أن:

$$(vS^m)\psi=(v\psi)T^m$$

وذلك لأي عدد صحيح $m\geq 0$. لذلك فإنه لأي كثيرة حدود $f(x)\in F[x]$ ولأي متجه $v\in V$ يكون

$$(vf(S))\psi=(v\psi)f(T)$$

إذا كان $F(S)=0$ فإن $(v\psi)f(T)=0$ لأي $v\in V$. ولما كان ψ يطبق V على W لذا يكون لدينا $Wf(T)=0$ ومن ثم فإن $f(T)=0$. وبالعكس إذا كانت $g(x)\in F[x]$ تحقق العلاقة $g(T)=0$. فإنه لأي $v\in V$ يكون $(vg(S))\psi=0$. ولما كان ψ تماثلا، لذلك فإن $vg(S)=0$ وهذا، بالطبع، يقتضي أن $g(S)=0$ وعليه فإن T و S يحققان نفس مجموعة كثيرات الحدود في $F[x]$ *ومن ثم فإنه يجب أن يكون لهما نفس كثيرة الحدود الدنيا*

$$p(x)=q_1(x)^{e1}q_2(x)^{e2}\ldots q_k(x)^{ek}$$

حيث $q_1(x),\ldots,q_k(x)$ كثيرات حدود مختلفة وغير مختزلة في $F[x]$.

إذا كان U فضاء متجهات جزئيا من V غير متغير بالنسبة لـ S فإن $U\psi$ فضاء متجهات جزئي من W غير متغير بالنسبة لـ T ذلك لأن

$$(U\psi)T=(US)\psi\subset U\psi$$

ولما كان U و $U\psi$ متماثلين لذا فإن كثيرة الحدود الدنيا لـ S_1 ، حيث S_1 هو التحويل الخطي المحدث بواسطة S على U ، هي نفسها كثيرة الحدود الدنيا لـ T_1 الذي هو التحويل الخطي المحدث بواسطة T على $U\psi$ وذلك وفقا للملاحظة الواردة آنفا.

الآن بما أن كثيرة الحدود الدنيا لـ S على V هي $p(x)=q_1(x)^{e_1}\ldots q_k(x)^{e_k}$ كما رأينا ذلك في المبرهنة (٦-٧-١) ونتيجتها، فإننا نستطيع أخذ $q_1(x)^{e_1}$ ليكون أول قاسم ابتدائي لـ S كما نستطيع إيجاد فضاء متجهات جزئي V_1 من V غير متغير بالنسبة لـ S بحيث إن:

١) $V=V_1+M$ حيث M غير متغير بالنسبة لـ S.

٢) القاسم الابتدائي الوحيد للتحويل الخطي S_1 المحدث بواسطة S على V_1 هو $q_1(x)^{e_1}$.

٣) القواسم الابتدائية الأخرى لـ S هي تلك القواسم الابتدائية للتحويل الخطي S_2 المحدث بواسطة S على M.

ومن هذا ندعي أن:

١) $W=W_1\oplus N$ حيث $W_1=V_1\psi$ و $N=M\psi$ غير متغيرين بالنسبة لـ T.

٢) إن القاسم الابتدائي الوحيد للتحويل الخطي T_1 المحدث بواسطة T على W_1 هو $q_1(x)^{e_1}$ *(الذي هو قاسم ابتدائي لـ T* لأن كثيرة الحدود الدنيا لـ T هي $p(x)=q_1(x)^{e_1}\ldots q_k(x)^{e_k}$).

٣) إن القواسم الابتدائية الأخرى لـ T هي تلك القواسم الابتدائية للتحويل الخطي T_2 المحدث بواسطة T على N.

لما كان $N=M\psi$ لذا فإن M و N فضاءا متجهات متماثلان على F وذلك بالنسبة للتماثل ψ_2 المحدث بواسطة ψ. وفضلا عن ذلك، فإنه إذا كان $u\in M$ فإن

$$(uS_2)\psi_2=(uS)\psi=(u\psi)T=(u\psi_2)T_2$$

لذلك فإن S_2 و T_2 على علاقة ببعضهما إزاء ψ_2 كما كان لـ S و T علاقة ببعضهما إزاء ψ. وباستخدام الاستقراء الرياضي على البعد (أو بتكرار المناقشة) نجد أن S_2 و T_2 لهما القواسم الابتدائية نفسها. ولكن لما كانت القواسم الابتدائية لـ S هي $q_1(x)^{e_1}$ بالإضافة إلى القواسم الابتدائية لـ T_2. بينما القواسم الابتدائية لـ T هي $q_1(x)^{e_1}$ بالإضافة إلى

القـواسم الابتـدائية لـ T_2 لذا فإننا نجد أنه يجب أن يكون لـ S و T نفس القواسم الابتدائية وبهذا يتم البرهان.

إن مبرهنة (٦ـ٧ـ١) ونتيجتها تعطينا الصيغة القانونية النسبية كما تنشأ تبعًا لها القواسم الابتدائية والآن نأتي إلى إثبات خاصة الوحدانية.

مبرهنة (٦ـ٧ـ٣)

يكون التحويلان الخطيان $S,T\in A_F(V)$ متشابهين إذا وفقط إذا كان لهما القواسم الابتدائية نفسها.

البرهان

إن أحد الاتجاهين بسيط لأنه إذا فرضنا أن لـ S و T القواسم الابتدائية نفسها فإنه ينتج عن ذلك وجود أساسين لـ V على F بحيث تكون مصفوفة S بالنسبة للأساس الأول تساوي مصفوفة T بالنسبة للأساس الثاني (وكل منهما تساوي مصفوفة الصيغة القانونية النسبية). ولكن، وفق ما رأينا سابقا في مناسبات عديدة، فإن هذا يقتضي تشابه S و T.

والآن إلى برهان الاتجاه المعاكس. إن المناقشة هنا تشبه إلى حد كبير تلك المناقشة الواردة في بند (٦ـ٥) عند إثبات مبرهنة (٦ـ٥ـ٢). وحيث إننا قد أوردنا ذلك البرهان مفصلاً لذا فإننا هنا نستطيع تقديمه باختصار.

أولا نلاحظ أنه بالنظر إلى مبرهنة (٦ـ٦ـ١) فإنه يمكننا تقليص المسألة من الحالة العامة إلى حالة التحويل الخطي الذي كثيرة حدوده الدنيا قوة لكثيرة حدود غير مختزلة. وبالتالي فإنه، بدون المساس بالحالة العامة، يمكننا أن نفرض أن كثيرة الحدود الدنيا لـ T هي $q(x)^e$ حيث $q(x)$ غير مختزلة من الدرجة d في $F[x]$.

إن الصيغة القانونية النسبية تفيد بإمكانية تفريق V على الصيغة

$$V=V_1\oplus\ldots\oplus V_r$$

وحيث كل فضاء متجهات جزئي V_i غير متغير بالنسبة لـ T ، كما أن مصفوفة التحويل الخطي المحدث بواسطة T على V_i هي $C(q(x)^e)$ أي المصفوفة المصاحبة لـ $q(x)^e$ ، إننا نحاول، في الحقيقة، برهان الآتي: إذا كان

$$V=U_1\oplus U_2\oplus\ldots\oplus U_s$$

حيث كل من U_j غير متغير بالنسبة لـ T وكانت مصفوفة التحويل الخطي المحدث بواسطة T على U_j هي $C(q(x)^{f_j})$ ، حيث $f_1\geqslant f_2\geqslant\ldots\geqslant f_s$. فإن

$$e_1=f_1,\ e_2=f_2,\ \ldots,\ e_r=f_r\ ;\ r=s$$

(أثبت أن برهان هذه العبارة مكافىء لبرهان المبرهنة).

لنفرض أنه لدينا التفريقين المذكورين أعلاه، أي

$$V=V_1\oplus\ldots\oplus V_r,\ V=U_1\oplus\ldots\oplus U_s$$

وأن $e_i\neq f_i$ لبعض قيم i. عندئذ يوجد عدد صحيح m بحيث يكون $e_m\neq f_m$ بينما $e_1=f_1,\ldots,e_{m-1}=f_{m-1}$ كما يمكن أن نفرض أن $e_m>f_m$.

الآن $g(T)^{f_m}$ تفني $U_m,U_{m+1},\ldots,U_s$ ومن ثم فإن:

$$Vq(T)^{f_m}=U_1q(T)^{f_m}\oplus\ldots\oplus U_{m-1}q(T)^{f_m}$$

ومع ذلك، فإنه يمكن إثبات أن بعد $U_iq(T)^{f_m}$ ، $i\leqslant m$ هو $d(f_i-f_m)$ (برهن ذلك!) ولذلك فإن

$$\dim(V_q(T)^{f_m})=d(f_1-f_m)+\ldots+d(f_{m-1}-f_m)$$

ومن ناحية أخرى،

$$Vq(T)^{f_m}\supseteq V_1q(T)^{f_m}\oplus\ldots\oplus V_mq(T)^{f_m}$$

ولما كان بعد $V_iq(T)^{f_m}$ هو $d(e_i-f_m)$ ، $i\leqslant m$ ، لذا فإننا نحصل على:

$$\dim\ (Vq(T)^{f_m})\geqslant d(e_i-f_m)+\ldots+d(e_m-f_m)$$

وحيث إن $e_m>f_m,\ e_1=f_1,\ldots,e_{m-1}=f_{m-1}$. لذا فإن هذا يناقض المساواة الواردة أعلاه. وبهذا يتم البرهان.

نتيجة

إذا كانت المصفوفتان $A,B\in F_n$ متشابهتين في K_n حيث K امتداد لـ F عندئذ فإن المصفوفتين A و B متشابهتان في F_n.

البرهان

لنفرض أن $A,B \in F_n$ بحيث أن $B=CAC^{-1}$ حيث $C \in K_n$. نعتبر هنا أن K_n يؤثر على $K^{(n)}$ الذي هو فضاء المتجهات للعديدات من رتبة n. عندئذ يكون $F^{(n)} \subset K^{(n)}$ ومع أن $F^{(n)}$ هو فضاء متجهات على F فإنه ليس فضاء متجهات على K. إنه ليس ضرورياً أن تقع صورة $F^{(n)}$ في $K^{(n)}$ تحت تأثير C مرة أخرى في $F^{(n)}$. ولكن، على أي حال، $F^{(n)}C$ مجموعة جزئية من $K^{(n)}$ الذي هو فضاء متجهات على F (برهن ذلك). ليكن V هو فضاء المتجهات $F^{(n)}$ على F و W هو فضاء المتجهات $F^{(n)}C$ على F ولنفرض أن $v\psi=vC$ حيث $v \in V$. الآن $A \in A_F(V)$ و $B \in A_F(W)$ كما أنه لأي $v \in V$ يكون:

$$(vA)\psi=vAC=vCB=(v\psi)B$$

ولهذا فإن شروط مبرهنة (٦-٧-٢) محققة. وعليه فإن لـ A و B القواسم الابتدائية نفسها، ووفقا لمبرهنة (٦-٧-٣) فإن A و B يجب أن تكونا متشابهتين في F_n.

تنبيـــــــــــه

إن النتيجة الآنفة الذكر لا تنص *على أنه* إذا كانت $A,B \in F_n$ وكانت $B=CAC^{-1}$ و $C \in K_n$ فإن من الضروري أن تكون $C \in F_n$ إن هذا غير صحيح. *إن ما تنص عليه هو أنه إذا كانت $A,B \in F_n$ بحيث أن $B=C^{-1}AC$ حيث $C \in K_n$ فإنه توجد مصفوفة D في F_n (قد تكون مختلفة عن C) بحيث أن $B=D^{-1}AD$.*

مســـائــل

١ - تحقق من أن V هو فضاء حلقي على $F[x]$ وفق التعريف المعطى.

٢ - برهن على أن جميع النقاط المشار إليها بـ «برهن على ذلك» والواردة في برهان مبرهنة (٦-٧-٣).

٣* - (ا) أثبت أن كل جذر لكثيرة الحدود المميزة لـ T هو جذر مميز لـ T.

(ب) برهن على أن تكرار أي جذر لـ $p_T(x)$ يساوي تكراره كجذر مميز لـ T.

٤ - أثبت أنه إذا كانت $f(x) \in F[x]$ فإن $C(f(x))$ تحقق $f(x)$ كما أن كثيرة الحدود الدنيا لـ $C(f(x))$ هي $f(x)$ وما هي كثيرة الحدود المميزة لـ $C(f(x))$ ؟

٥ - إذا كان F هو حقل الأعداد النسبية. فأوجد جميع الصيغ القانونية النسبية الممكنة وكذلك القواسم الابتدائية لكل مما يأتي:

(ا) المصفوفات من النوع 6×6 في F_6 التي كثيرة حدودها الدنيا هي $(x-1)(x^2+1)^2$.

(ب) المصفوفات من النوع 15×15 في F_{15} التي كثيرة حدودها الدنيا هي $(x^2+x+1)^2(x^3+2)^2$.

(جـ) المصفوفات من النوع 10×10 في F_{10} التي كثيرة حدودها الدنيا هي $(x^2+1)^2(x^3+1)$.

٦ - (ا) إذا كان K هو امتداد F وكانت $A\in K_n$. فأثبت أنه يمكن كتابة A على الصيغة $A=\lambda_1A_1+\ldots+\lambda_kA_k$، حيث $A_1,\ldots,A_k\in F_n$، كما أن $\lambda_1,\ldots,\lambda_k\in K$ مستقلة خطيًّا على F.

(ب) على افتراض أن الترميز الوارد هنا هو كما في الفقرة (ا). أثبت أنه إذا كانت $B\in F_n$ بحيث أن $AB=0$ فإن $A_1B=A_2B=\ldots=A_kB=0$.

(جـ) إذا كانت C تتبادل مع A فأثبت أنها تتبادل مع كل من $A_1,\ldots,A_k$.

٧* - إذا كانت $A_1,\ldots,A_k\in F_n$ وذلك لبعض قيم $\lambda_1,\ldots,\lambda_k\in K$، حيث K هو امتداد F وكان لـ $\lambda_1A_1+\ldots+\lambda_kA_k$ معكوس في K_n، فأثبت أنه إذا كان F يحتوي على عدد غير منته *من العناصر* فإن باستطاعتنا إيجاد $\alpha_1,\ldots,\alpha_k\in F$ بحيث يكون لـ $\alpha_1A_1+\ldots+\alpha_kA_k$ معكوس في F_n.

٨* - إذا كان F حقلا *منتهيا* فأثبت أن نتيجة المسألة (٧) غير صحيحة.

٩* - باستخدام نتيجتي المسألتين ٦(أ) و(٧). أثبت أنه إذا كان F يحتوي على عدد غير منته من العناصر فإنه إذا كانت $A,B\in F_n$ متشابهتين في K_n حيث K هو امتداد F فإنهما متشابهتان في F_n. (إن هذا يزودنا ببرهان مستقل عن الصيغة القانونية للنتيجة الأولى لمبرهنة (٦-٧-٣) وذلك في الحالة التي يكون فيها F حقلا غير منته).

١٠ - باستخدام حسابات مصفوفية (ولكن باتباع ما ورد في مسألة (٩)). أثبت أنه إذا كان F هو حقل الأعداد الحقيقية و K هو حقل الأعداد المركبة فإن أي عنصرين من F_2 اللذين هما متشابهان في K_2 يكونان بالفعل متشابهين في F_2.

(٦ـ٨) الأثـــر والمنقـــول

إن الطبيعة غير المعقدة للمادة التي سنتناولها في هذا البند يمكن اعتبارها راحة ذهنية بعد الدراسة المكثفة الواردة في البنود القليلة السابقة.

ليكن F حقلا و A مصفوفة في F_n.

تعريف

*نعرف **أثر** (Trace) المصفوفة A بأنه مجموع العناصر في القطر الرئيس فيها.*

سنرمز لأثر المصفوفة A بالرمز trA ، فإذا كانت $A=(\alpha_{ij})$ فإن

$$trA=\sum_{i=1}^{n}\alpha_{ii}$$

إن الخواص الأساسية لدالة الأثر تتلخص فيما يلي:

تمهيدية (٦ـ٨ـ١)

إذا كانت $A,B\in F_n$ و $\lambda\in F$ فإن:

(١) $tr(\lambda A)=\lambda trA$

(٢) $tr(A+B)=trA+trB$

(٣) $tr(AB)=tr(BA)$

البرهان

إن برهان (١)، (٢) [والذي يؤكد على أن الأثر عبارة عن دالي خطي على F_n] بسيط لذلك نتركه للقارىء ومن ثم فإننا نبرهن القسم الثالث من التمهيدية.

إذا كانت $A=(\alpha_{ij})$ و $B=(\beta_{ij})$ فإن $AB=(\gamma_{ij})$ حيث

$$\gamma_{ij}=\sum_{k=1}^{n}\alpha_{ik}\beta_{kj}$$

كما أن $BA=(\mu_{ij})$ حيث

$$\mu_{ij}=\sum_{k=1}^{n}\beta_{ik}\alpha_{kj}$$

وهكذا فإن

$$tr(AB)=\sum_i\gamma_{ii}=\sum_i(\sum_k\alpha_{ik}\beta_{ki})$$

وبمبادلة ترتيب الجمع في علاقة الجمع الأخيرة نحصل على

$$tr(AB)=\sum_{k=1}^{n}\sum_{i=1}^{n}\alpha_{ik}\beta_{ki}=\sum_{k=1}^{n}(\sum_{i=1}^{n}\beta_{ki}\alpha_{ik})=\sum_{k=1}^{n}\mu_{kk}=tr(BA)$$

نتيجة

إذا كان يوجد للمصفوفة A معكوس فإن $tr(ACA^{-1})=trC$.

البرهان

لنفرض أن $B=CA^{-1}$ عندئذ

$$tr(ACA^{-1})=tr(AB)=tr(BA)=tr(CA^{-1}A)=trC$$

إن لهذه النتيجة أهميتين: **أولاهما** أنها تسمح لنا بتعريف الأثر لأي تحويل خطي. **والثانية** أنها تمكننا من إيجاد صيغة بديلة لأثر A.

تعريف

*إذا كان $T\epsilon A(V)$ فإن trT أي **أثـر** T يعرف بأنه أثر $m_1(T)$ حيث $m_1(T)$ هي مصفوفة T بالنسبة لأساس ما لـ V.*

إن أثر T يعتمد على T وليس على أي أساس معيّن لـ V. ذلك أنه إذا كانت $m_1(T)$ و $m_2(T)$ هما مصفوفتا T بالنسبة لأساسين مختلفي لـ V، فإنه وفقا لمبرهنة (٦-٣-٢) تكون المصفوفتان $m_1(T)$ و $m_2(T)$ متشابهتين ووفقا لنتيجة التمهيدية (٦-٨-١) يكون لهما الأثر نفسه.

تمهيدية (٦-٨-٢)

إذا كان $T\epsilon A(V)$ فإن trT هو مجموع الجذور المميزة لـ T (وذلك باستخدام كل جذر مميز بمقدار تكراره).

البرهان

هنا يمكن أن نفرض أن T مصفوفة في F_n ، وإذا كان K هو حقل انشطار كثيرة الحدود الدنيا لـ T على F ، فإنه يمكن تحويل T في K_n وفقا لمبرهنة (٦-٦-٢) إلى صيغة جوردان J. إن J هي المصفوفة التي تظهر على قطرها الجذور المميزة لـ T ، كما أن كل جذر يظهر متكررا بمقدار تكراره. وهكذا فإن trT يساوي مجموع الجذور المميزة لـ T ، ومع ذلك فإن J من الصيغة ATA^{-1} ولهذا فإن trJ=trT مما يثبت التمهيدية.

إذا كان T معـدوم القـوى فإن جميع جذوره المميزة أصفار. ومن ثم فإنه وفقا لتمهيدية (٦-٨-٢) يكون trT=0. ولكن إذا كان T معدوم القوى فكذلك يكون $T^2, T^3, \ldots,$ وهكذا فإن $trT^i=0$ لكل i ، $i \geqslant 1$.

والآن، ماذا عن الاتجـاه الآخـر؟ أي إذا كان $trT^i=0$ حيث $i=1,2,\ldots,$ فهـل نستنتج من ذلك أن T معدوم القوى؟ كلا، لأنه إذا كان مميز الحقل F يساوي 2 فإن أثر مصفوفة الوحدة في F_2 التي هي

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

يساوي الصفر (لأن 1+1=0) وهكذا بالنسبة لجميع قواها. ومن الواضح، أن مصفوفة الوحدة ليست معدومة القوى، ومع ذلك، فإنه إذا كان مميز الحقل يساوي صفرًا فإن النتيجة صحيحة بالفعل.

تمهيدية (٦-٨-٣)

إذا كان مميز الحقل F يساوي صفرًا وكان $T \in A_F(V)$ بحيث أن $trT^i=0$ لكل $i \geqslant 1$ فإن T معدوم القوى.

البرهان

لما كان $T \in A_F(V)$ ، فإن T يحقق كثيرة حدود دنيا $p(x)=x^m+\alpha_1 x^{m-1}+\ldots+\alpha_m$.
وبأخذ الأثر لطرفي المعادلة

$$T^m+\alpha_1 T^{m-1}+\ldots+\alpha_{m-1}T+\alpha_m=0$$

نحصل على

$$trT^m+\alpha_1 trT^{m-1}+\ldots+\alpha_{m-1}trT+trT\alpha_m=0$$

ولكن $trT^i=0$ لكل $i\geq 1$ ، لهذا نتوصل إلى أن $tr\alpha_m=0$ فإذا كان $\dim V=n$ ، فإن $tr\alpha_m=n\alpha_m$. ومن ثم فإن $n\alpha_m=0$. ولكن مميز F يساوي صفرًا. لذلك فإن $n\neq 0$ ومنه ينتج أن $\alpha_m=0$. ولما كان الحد الثابت في كثيرة الحدود الدنيا يساوي صفرًا. لذا فإنه استنادا إلى مبرهنة (٦-١-٢) يكون T شاذًا وبناء عليه فإن الصفر يكون جذرًا مميزًا لـ T.

الآن ننظر إلى T باعتباره مصفوفة في F_n. ومن ثم فإنه مصفوفة في K_n حيث K هو امتداد F الذي بدوره يحتوي على جميع الجذور المميزة لـ T. وفقا لمبرهنة (٦-٤-١) نستطيع تحويل T إلى الصيغة المثلثة في K_n. ولما كان الصفر جذرًا مميزًا لـ T ، فإننا في الواقع نستطيع تحويل T إلى الصيغة

$$\left(\begin{array}{c|cccc} 0 & 0 & . & \ldots & 0 \\ \hline \beta_2 & \alpha_2 & 0 & \ldots & 0 \\ \vdots & & & \cdot & \vdots \\ \beta_n & * & & & \alpha_n \end{array}\right) = \left(\begin{array}{c|c} 0 & 0 \\ \hline * & T_2 \end{array}\right),$$

حيث

$$T_2=\begin{pmatrix} \alpha_2 & 0 & 0 \\ & \ddots & \vdots \\ & * & \alpha_n \end{pmatrix}$$

هي مصفوفة من النوع $(n-1)\times(n-1)$ (إن * هي عبارة عن العناصر في المصفوفة والتي ليست لها أهمية بالنسبة لنا). الآن

$$T^k=\left(\begin{array}{c|c} 0 & 0 \\ \hline * & T_2^k \end{array}\right)$$

ولذلك فإن $0=trT^k=trT_2^k$. وهكذا فإن T_2 مصفوفة من النوع $(n-1)\times(n-1)$ والتي تحقق $trT_2^k=0$ لكل k حيث $k\geq 1$. باستخدام الاستقراء على n أو بتكرار المناقشة نفسها التي

استخدمت في T على T_2. نجد أن $\alpha_2=\ldots=\alpha_n=0$ لأن $\alpha_2,\ldots,\alpha_n$ هي الجذور المميزة لـ T_2. وهكذا فإنه عندما يتم تحويل T إلى الصيغة المثلثة فإن جميع عناصره التي في القطر الرئيس أصفار مما يجبر T على أن يكون معدوم القوى. (أثبت ذلك).

إن لهذه التمهيدية، على الرغم من أنها تبدو كحالة خاصة، استعمالات عديدة وسنوظفها مباشرةً في إثبات النتيجة التالية المعروفة عادة بتمهيدية جيكوبسون (Jacobson).

تمهيدية (٦ـ٨ـ٤)

إذا كان مميز F يساوي صفرًا وكان $T,S\in A_F(V)$ بحيث أن $ST-TS$ يتبادل مع S فإن $ST-TS$ معدوم القوى.

البرهان

بحساب $(ST-TS)^k$ لأي k ، $k\geq1$ نجد

$$(ST-TS)^k=(ST-TS)^{k-1}(ST-TS) =(ST-TS)^{k-1}ST-(ST-TS)^{k-1}TS$$

ولما كان $ST-TS$ يتبادل مع S ، فإنه يمكن كتابة الحد $(ST-TS)^{k-1}ST$ على الصيغة $S((ST-TS)^{k-1}T)$. لنفرض الآن أن $B=(ST-TS)^{k-1}T$ عندئذ نجد أن $(ST-TS)^k=SB-BS$ لذلك فإن

$$tr((ST-TS)^k)=tr(SB-BS)=tr(SB)-tr(BS)=0$$

وذلك وفقا لتمهيدية (٦ـ٨ـ١). واستنادا إلى التمهيدية السابقة فإن $ST-TS$ يجب أن يكون معدوم القوى.

إن الأثر هو دالي خطي بالغ الفائدة من F_n (ومن ثم، من $(A_F(V))$ إلى F. ننتقل الآن إلى تقديم تطبيق مهم من F_n إلى نفسها.

تعريف

إذا كانت $A=(\alpha_{ij})\in F_n$ ، فإن منقول (Transpose) A ويكتب A' هو المصفوفة $A'=(\gamma_{ij})$ ، حيث $\gamma_{ij}=\alpha_{ji}$ لكل i ولكل j.

إن منقـول A هو المصفوفة الناتجة من مبادلة صفوف وأعمدة المصفوفة A. إن الخواص الأساسية للمنقول تتضمنها التمهيدية الآتية.

تمهيدية (٦ـ٨ـ٥)

لكل $A,B\in F_n$ يكون:

(١) $(A')'=A$

(٢) $(A+B)'=A'+B'$

(٣) $(AB)'=B'A'$

البرهان

إن برهان الفقرتين الأولى والثانية بسيط ولذلك فهو متروك للقارىء. والآن نثبت الفقرة الثالثة.

لنفرض أن $A=(\alpha_{ij})$ و $B=(\beta_{ij})$، عندئذ $AB=(\lambda_{ij})$، حيث

$$\lambda_{ij}=\sum_{k=1}^{n}\alpha_{jk}\beta_{kj}$$

ولذلك فإنه وفقا لتعريف المنقول يكون، $(AB)'=(\mu_{ij})$، حيث

$$\mu_{ij}=\lambda_{ji}=\sum_{k=1}^{n}\alpha_{jk}\beta_{ki}$$

ومن ناحية أخرى، $A'=(\gamma_{ij})$ حيث $\gamma_{ij}=\alpha_{ji}$ و $B'=(\xi_{ij})$ حيث $\xi_{ij}=\beta_{ji}$. ولهذا فإن العنصر في الموقع (i,j) من $B'A'$ هو

$$\sum_{k=1}^{n}\xi_{ik}\gamma_{kj}=\sum_{k=1}^{n}\beta_{ki}\alpha_{jk}=\sum_{k=1}^{n}\alpha_{jk}\beta_{ki}=\mu_{ij}$$

أي أن $(AB)'=B'A'$ وبهذا نكون قد برهنا الفقرة الثالثة من التمهيدية.

بوضع $B=A$ في الفقرة الثالثة نحصل على $(A^2)'=(A')^2$. بالاستمرار على هذا النحو نحصل على $(A^k)'=(A')^k$ وذلك لجميع الأعداد الصحيحة الموجبة k. وعندما يوجد معكوس لـ A فإن $(A^{-1})'=(A')^{-1}$. هناك خاصة إضافية أخرى للمنقول وهي أنه إذا كان $\lambda\in F$ فإن $(\lambda A)'=\lambda A'$ لكـــل $A\in F_n$. الآن إذا كانـــت $A\in F_n$ تحقـــق كثـــيرة

الحدود $\alpha_0A^m+\alpha_1A^{m-1}+\ldots+\alpha_m=0$ ، فإننا نحصل على $(\alpha_0A^m+\ldots+\alpha_m)'=0'=0$
وبحساب $(\alpha_0A^m+\ldots+\alpha_m)'$ باستعمال خواص المنقول نحصل على

$$\alpha(A')^m+\alpha_1(A')^{m-1}+\ldots+\alpha_m=0$$

مما يعني أن A' تحقق أي كثيرة حدود محققة بواسطة A. ولما كان $A=(A')'$ فإنه بالطريقة نفسها نجد أن A تحقق أي كثيرة حدود محققة بواسطة A'. وبصورة خاصة فإن A و A' يحققان كثيرة الحدود الدنيا نفسها على F. ومن ثم فإن لهما الجذور المميزة نفسها. إن بإمكاننا إثبات أن كل جذر له التكرار نفسه في A و A'. إن هذا واضح، ذلك لأنه يمكن إثبات أن A و A' متشابهتان (انظر مسألة ١٤).

تعريف

*يقال إن المصفوفة A هي **مصفوفة متناظرة** (symmetric matrix) إذا كان $A'=A$.*

تعريف

*يقال عن المصفوفة A إنها **مصفوفة متناظرة تخالفيا** (skew-symmetric) إذا كان $A'=-A$.*

إنه لن يكون باستطاعتنا التمييز بين المصفوفات المتناظرة والمتناظرة تخالفيًا وذلك في حالة كون مميز الحقل F يساوي 2 ذلك لأن $1=-1$. **ولهذا فإننا سنفترض فيما تبقى من هذا البند أن مميز F لا يساوي 2.**

إن لدينا طرقًا للحصول على مصفوفات متناظرة ومتناظرة تخالفيا. فعلى سبيل المثال، إذا كانت A مصفوفة ما فإن $A+A'$ مصفوفة متناظرة كما أن $A-A'$ متناظرة تخالفيا. لاحظ أن $A=\frac{1}{2}(A+A')+\frac{1}{2}(A-A')$. إن أية مصفوفة هي عبارة عن مجموع مصفوفتين إحداهما متناظرة والأخرى متناظرة تخالفيا. إن هذا التفريق وحيد (انظر مسألة ١٩). طريقة أخرى للحصول على المصفوفات المتناظرة يمكن وصفها كما يلي: إذا كانت A مصفوفة معيّنة، فإن AA' و $A'A$ متناظرتان. (لاحظ أنه ليس من الضروري تساويهما).

إن من طبيعة المشتغل بالرياضيات هي أنه متى ما واجه مفهومًا مهمًا ناشئًا من وضع خاص، فإنه يحاول تجريد هذا المفهوم من خصوصيته ويوظف الخواص الأساسية

لهذا المفهـوم كوسـائل لتجريده. والآن نتبع هذه الطريقة مع المنقول. لذلك نأخذ الخواص الأساسية للمنقول الواردة في نص تمهيدية (٦ـ٨ـ٥) والتي تؤكد على أن المنقول يعرف **تماثلا ذاتيا مضادا** (anti-automorphism) دورته تساوي 2 على F_n. إن هذا يقود إلى التعريف الآتي.

تعريف

*إن التطبيق * من F_n إلى F_n يدعى **تطبيقًا قرينًا** (adjoint) على F_n إذا كان*

(١) $(A^*)^*=A$

(٢) $(A+B)^*=A^*+B^*$

(٣) $(A\,B)^*=B^*A^*$

لاحظ هنا أننا لا نصر على أن يكون $(\lambda A)^*=\lambda A^*$ ، حيث $\lambda\in F$. وفي الحقيقة فإن هذه ليست هي الحالة في معظم القرائن المستخدمة ولنناقش الآن واحدا منها. ليكن F هو حقل الأعداد المركبة ولنفرض أن $A=(\alpha_{ij})\in F_n$. عندئذ $A^*=(\lambda_{ij})$ حيث $\gamma_{ij}=\bar{\alpha}_{ji}$ هـو الـمرافق الـمركب للعدد α_{ji}. إن التطبيق * يدعى، في هذه الحالة، **بالقرين الـهرميتي** (Hermitian Adjoint) على F_n. وفي بنود لاحقة سندرس بالتفصيل بعض المصفوفات بالنسبة للقرين الهرميتي.

إن كل شيء ذكرناه حول المنقول، مثل التناظر، التناظر التخالفي ينسحب على القرائن العامة. ونتحدث عن العناصر المتناظرة تحت تأثير * (فمثلا $A^*=A$) والعناصر المتناظرة تخالفيا تحت تأثير * الخ . . . وفي نهاية هذا البند توجد أمثلة ومسائل عديدة متعلقة بالقرائن العامة.

دعنا ندرس القرين الهرميتي. إننا لن نسمي أية معلومات نحصل عليها مبرهنة، ليس هذا بسبب أنها لا تستحق هذا العنوان ولكن لأننا سنعيد عمل ذلك (وسنميزه تماما) من وجهة نظر مركزية.

لنفرض أن F هو حقل الأعداد المركبة وأن القرين على F_n هو القرين الهرميتي. يقال عن المصفوفة A إنها هرميتية إذا كان $A^*=A$.

الملاحظة الأولى هي أنه إذا كان $0\neq A\in F_n$ فإن $tr(AA^*)>0$. **والملاحظة الثانية** هي أنه نتيجة للملاحظة الأولى إذا كان $A_1,...,A_k\in F_n$ وإذا كان $A_1A_1^*+A_2A_2^*+...+A_kA_k^*=0$ فإن $A_1=A_2=...=A_k=0$. **والملاحظة الثالثة** هي أنه إذا كانت λ مصفوفة قياسية فإن $\lambda^*=\bar{\lambda}$ المرافق المركب لـ λ.

لنفرض أن $A\in F_n$ هرميتية وأن العدد المركب $\alpha+\beta i$ ، حيث α و β حقيقيان و $i^2=-1$ ، هو جذر مميز لـ A. عندئذ ليس للمصفوفة $A-(\alpha+\beta i)$ معكوس. وعندئذ فإنه لا يوجد للمصفوفة $(A-(\alpha+\beta i))(A-(\alpha-\beta i))$ معكوس. بيد أنه إذا كانت هناك مصفوفة شاذة فإنها يجب أن تفني مصفوفة غير صفرية (مبرهنة ٦-١-٢ ونتيجتها رقم ٢). ولذلك فإنه يجب أن توجد مصفوفة $C\neq 0$ بحيث أن $C((A-\alpha)^2+\beta^2)=0$. بالضرب من اليمين بـ C^* نحصل على:

$$C(A-\alpha)^2C^*+\beta^2CC^*=0 \qquad (١)$$

لتكن $D=C(A-\alpha)$ و $E=\beta C$. بما أن $A^*=A$ وبما أن α عدد حقيقي فإن $C(A-\alpha)^2C^*=DD^*$. وبما أن β عدد حقيقي فإن $\beta^2CC^*=EE^*$. وهكذا فإن المعادلة (١) تصبح $DD^*+EE^*=0$. ومن الملاحظات الواردة أعلاه فإن هذا يستلزم أن تكون $D=0$ و $E=0$. الآن ندرس العلاقة $E=0$. بما أن $0=E=\beta C$ وبما أن $C\neq 0$ فإنه يجب أن يكون لدينا $\beta=0$. تُرى ما هو الشيء الذي أثبتناه؟ في الحقيقة لقد برهنا النتيجة (المهمة) التي تنص على أنه *إذا كان العدد المركب λ جذرا مميزًا لمصفوفة هرميتية فإن λ ، عندئذ، يجب أن يكون عددًا حقيقيًا*. وباستخدام خواص الأعداد المركبة يمكن كتابة نص هذه النتيجة كما يلي: *إن الجذور المميزة للمصفوفة الهرميتية جميعها حقيقية*.

الآن نواصل نقاشنا على هذا النهج. لتكن $B=AA^*$ حيث $A\in F_n$. ، إن B مصفوفة هرميتية. إذا كان العدد الحقيقي α جذرًا مميزًا لـ B فهل يمكن أن يكون α أي عدد حقيقي أو أنه يجب أن يكون مقيدا بطريقة ما؟ إننا ندعي، بالفعل، أن α يجب أن يكون غير سالب، لأنه إذا كان α سالبا فإن $\alpha=-\beta^2$ حيث β عدد حقيقي. ولكن، عندئذ، لا يوجد معكوس للمصفوفة $B-\alpha=B+\beta^2=AA^*+\beta^2$ ومن هنا فإنه يوجد مصفوفة $C\neq 0$ بحيث يكون $C(AA^*+\beta^2)=0$. بالضرب بـ C^* من اليمين وتكرار المناقشة السابقة نحصل على $\beta=0$ وهذا تناقض. بهذا نكون قد برهنا على أن أي جذر مميز

حقيقيُ للمصفوفة AA^* يجب أن يكون غير سالب وفي الحقيقة أن كلمة «حقيقي» في هذه العبارة غير ضرورية إذ أنه يمكن أن نكتب العبارة كما يلي: إن جميع الجذور المميزة للمصفوفة AA^* غير سالبة وذلك لأية مصفوفة $A\in F_n$.

مسائل

إن التناظر والتناظر التخالفي سيكون بالنسبة للمنقول ما لم ينص على غير ذلك.

١ - برهن على أن $tr(A+B)=trA+trB$ وأن $tr(\lambda A)=\lambda trA$ حيث $\lambda\in F$.

٢ - (ا) أثبت باستخدام الأثر أنه إذا كان مميز F يساوي صفرًا فإن من غير الممكن إيجاد مصفوفتين $A,B\in F_n$ بحيث إن $AB-BA=1$.

(ب) في الفقرة (ا) برهن، في الحقيقة، على أن $1-(AB-BA)$ لا يمكن أن تكون معدومة القوى.

٣ - (ا) لتكن f دالة معرفة على F_n بحيث تكون قيمها في F تحقق ما يلي:

$$f(A+B)=f(A)+f(B) \qquad (١)$$

$$f(\lambda A)=\lambda f(A) \qquad (٢)$$

$$f(AB)=f(BA) \qquad (٣)$$

لكل $A,B\in F_n$ ولكل $\lambda\in F$. برهن على أنه يوجد عنصر $\alpha_0\in F$ بحيث يكون $f(A)=\alpha_0 trA$ لكل $A\in F_n$.

(ب) إذا كان مميز F يساوي صفرًا وإذا كانت f الواردة في (ا) تحقق خاصة إضافية هي $f(1)=n$. فأثبت أن $f(A)=trA$ لكل $A\in F_n$.

لاحظ أن المسألة (٣) تميز دالة الأثر.

٤* - (ا) إذا كان الحقل F يحتوي على عدد غير منته من العناصر. فأثبت أنه يمكن كتابة كل عنصر في F_n على هيئة مجموع مصفوفات منتظمة.

(ب) إذا كان F يحتوي على عدد غير منته من العناصر وكانت الدالة f المعرفة على F_n بقيم في F تحقق الخواص الآتية.

$$f(A+B)=f(A)+f(B) \qquad (١)$$

(٢) $f(\lambda A)=\lambda f(A)$

(٣) $f(BAB^{-1})=f(A)$

لكل $A\in F_n$ ولكل $\lambda\in F$ ولكل عنصر B له معكوس في F_n. فأثبت أن $f(A)=\alpha_0 tr(A)$ وذلك لعنصر معيّن $\alpha_0\in F$ ولكل $A\in F_n$.

٥ - برهن تمهيدية جيكوبسون للعنصرين $A,B\in F_n$ إذا كان n أقل من مميز F.

٦ - (ا) لنعرف التطبيق d_c، حيث $C\in F_n$ ، على F_n بالقاعدة $d_C(X)=XC-CX$ حيث $X\in F_n$. أثبت أن

$$d_C(XY)=(d_C(X))Y-X(d_C(Y))$$

(هل يذكرك هذا بالمشتق)؟

(ب) باستخدام (ا). أثبت أنه إذا كانت AB–BA تتبادل مع A فإنه لأي كثيرة حدود $q(x)\in F[x]$ يكون $q(A)B-Bq(A)=q'(A)(AB-BA)$ حيث $q'(x)$ هو مشتق $q(x)$.

٧* - استخدم فقرة (ب) في مسألة (٦) لتبرهن تمهيدية جيكوبسون. (**إرشاد**: لتكن $p(x)$ هي كثيرة الحدود الدنيا لـ A ثم اعتبر: $0=p(A)B-Bp(A)$).

٨ - (ا) إذا كانت A مصفوفة مثلثة. فأثبت أن العناصر في القطر الرئيس في A هي الجذور المميزة لـ A.

(ب) إذا كانت A مثلثة وكانت العناصر في القطر الرئيس أصفارًا. فأثبت أن A معدومة القوى.

٩ - برهن على أنه لأي $A,B\in F_n$ ولأي $\lambda\in F$ يكون $A=(A')'$ و $(A+B)'=A'+B'$ و $(\lambda A)'=\lambda A'$.

١٠ - إذا كان يوجد معكوس للمصفوفة A. فأثبت أن $(A^{-1})'=(A')^{-1}$.

١١ - إذا كانت A متناظرة تخالفيًا. فأثبت أن جميع العناصر في قطرها الرئيس أصفارًا.

١٢ - إذا كانت كل من A و B متناظرة. فأثبت أن AB متناظرة إذا وفقط إذا كان $AB=BA$.

١٣ - أورد مثالا لمصفوفة A بحيث تكون $AA'\neq A'A$.

١٤* - أثبت أن A و A' متشابهتان.

١٥ - إن العناصر المتناظرة في F_n تشكل فضاء متجهات. أوجد أساسا له ثم أوجد بعده.

١٦* - لنفرض أن S ترمز إلى مجموعة العناصر المتناظرة في F_n. أثبت أن الحلقة الجزئية من F_n والمولدة بـ S هي جميع F_n.

١٧* - إذا كان مميز F صفرًا وكان $tr(A)=0$ حيث $A\in F_n$. فأثبت أنه يوجد $C\in F_n$ بحيث تكون العناصر في القطر الرئيس في CAC^{-1} أصفارًا فقط.

١٨* - إذا كان مميز F يساوي صفرًا وكان أثر $A\in F_n$ يساوي صفرًا. فأثبت أنه توجد $B,C\in F_n$ بحيث يكون $A=BC-CB$ (**إرشاد**: الخطوة الأولى: افرض وفقا لنتيجة المسألة (١٧) أن جميع العناصر في القطر الرئيس للمصفوفة A هي أصفار).

١٩ - (ا) إذا كان مميز F لا يساوي 2 وإذا كان * أي قرين على F_n وإذا كانت $S=\{A\in F_n | A^*=A\}$ و $K=\{A\in F_n | A^*=-A\}$ فأثبت أن: $S+K=F_n$.

(ب) إذا كانت $A\in F_n$ وكانت $A=B+C$ ، $B\in S$ و $C\in K$ فأثبت أن كلا من B و C وحيدة ثم عيِّنهما.

٢٠ - (ا) إذا كانت $A,B\in S$. فأثبت أن $AB+BA\in S$

(ب) إذا كانت $A,B\in K$. فأثبت أن $AB-BA\in K$

(جـ) إذا كانت $A\in S$ و $B\in K$. فأثبت أن $AB-BA\in S$ وأن $AB+BA\in K$.

٢١ - إذا كان ϕ تماثلاً ذاتيًا على الحقل F وعرفنا التطبيق Φ على F_n كما يلي: إذا كانت $A=(\alpha_{ij})$ فإن $\Phi(A)=(\phi(\alpha_{ij}))$. أثبت أن $\Phi(A+B)=\Phi(A)+\Phi(B)$ وأن $\Phi(AB)=\Phi(A)\Phi(B)$ لكل $A,B\in F_n$.

٢٢ - إذا كان * و ⊛ يعرفان قرينين على F_n. فأثبت أن التطبيق $\psi:A\to(A^*)^{⊛}$ لكل A في F_n يحقق العلاقة $\psi(A+B)=\psi(A)+\psi(B)$ وأن $\psi(AB)=\psi(A)\psi(B)$ لكل A و B في F_n.

٢٣ - إذا كان * هو أي قرين على F_n و λ مصفوفة قياسية في F_n. فأثبت أن λ^* يجب أن تكون مصفوفة قياسية.

٢٤* ـ لنفرض معرفة المبرهنة الآتية: إذا كان ψ تماثلاً ذاتيًا على F_n (أي أن ψ يطبق F_n على نفسها بطريقة يكون فيها $\psi(A+B)=\psi(A)+\psi(B)$ و $\psi(AB)=\psi(A)\psi(B)$) بحيث يكون $\psi(\lambda)=\lambda$ لكل مصفوفة قياسية λ، عندئذ يوجد عنصر $P\in F_n$ بحيث يكون $\psi(A)=PAP^{-1}$ لكل $A=F_n$. أثبت، استنادا إلى هذه المبرهنة، أنه إذا كان * قرينًا على F_n بحيث يكون $\lambda^*=\lambda$ لكل مصفوفة قياسية λ فإنه، عندئذ، يوجد مصفوفة $P\in F_n$ بحيث يكون $A^*=PA'P^{-1}$ لكل مصفوفة $A\in F_n$ وفضلا عن ذلك فإن $P^{-1}P'$ يجب أن تكون قياسية.

٢٥ ـ إذا كان $P\in F_n$ بحيث أن $0\neq P^{-1}P'$ مصفوفة قياسية. فأثبت أن التطبيق المعرف بالقاعدة $A^*=PA'P^{-1}$ هو قرين على F_n.

٢٦* ـ بافتراض معرفة المبرهنة الواردة حول التماثل الذاتي في مسألة (٢٤). أثبت ما يلي: إذا كان * قرينا على F_n فإنه يوجد تماثل ذاتي ϕ على F دورته تساوي 2 وعنصر $P\in F_n$ بحيث يكون لكل $A\in F_n$ ، $A^*=P(\Phi(A))'P^{-1}$ (راجع مسألة (٢١) من أجل الاصطلاح)، وفضلا عن ذلك أثبت أن $P^{-1}\Phi(P)'$ هي مصفوفة قياسية.

إن المسألتين (٢٤) و (٢٦) تدلان على أن القرين العام على F_n ليس منفصلا عن المنقول وذلك كما يتضح من أول نظرة.

٢٧* ـ إذا كانت ψ تشاكلاً ذاتيًا لـ F_n بحيث أن $\psi(\lambda)=\lambda$ لجميع القياسات λ، برهن على أنه يوجد P في F_n بحيث إن $\psi(A)=PAP^{-1}$ لكل A في F_n.

فيما تبقى من المسائل سيكون F هو حقل الأعداد المركبة كما أن * هو القرين الهرميتي.

٢٨ ـ إذا كانت $A\in F_n$. فأثبت أنه يوجد مصفوفتان هرميتيتان وحيدتان B و C بحيث يكون $A=B+iC$ $(i^2=-1)$.

٢٩ ـ أثبت أنه إذا كانت $A\neq 0$ فإن $trAA^*>0$.

٣٠ ـ باستخدام حساب عناصر المصفوفة مباشرة. أثبت أنه إذا كان $A_1A_1^*+\ldots+A_kA_k^*=0$ فإن

$$A_1=A_2=\ldots=A_k=0.$$

٣١ - إذا كانت $A \in F_n$ وكانت $BAA^*=0$. فأثبت أن $BA=0$.

٣٢ - إذا كانت المصفوفة $A \in F_n$ هرميتية وكان $BA^k=0$ فأثبت أن $BA=0$.

٣٣ - إذا كانت $A \in F_n$ هرميتية وكان λ, μ جذرين مميزين مختلفين (حقيقيين) لـ A وكان $C(A-\lambda)=0$ و $D(A-\lambda)=0$ ، فأثبت أن $CD^*=DC^*=0$.

*٣٤ - (ا) على افتراض أن جميع الجذور المميزة للمصفوفة الهرميتية A تقع في حقل الأعداد المركبة ومن نتائج المسألتين (٣٢) و(٣٣) وحقيقة أن الجذور، عندئذ، يجب أن تكون حقيقية وبالاستعانة بنتيجة المبرهنة (٦-٦-١). أثبت أنه يمكن تحويل A إلى الصيغة القطرية، بمعنى أنه توجد مصفوفة P بحيث تكون PAP^{-1} قطرية.

(ب) في الفقرة (ا). أثبت أنه يمكن اختيار P بحيث تكون $PP^*=1$.

٣٥ - لتكن $V_n=\{A \in F_n | AA^*=1\}$. أثبت أن V_n مع عملية ضرب المصفوفات هي زمرة.

٣٦ - إذا كانت A تتبادل مع AA^*-A^*A. فأثبت أن $AA^*=A^*A$

(٦-٩) المحـــــددات

إن الأثـر يعـرف دالـة مفيدة من حلقـة المصفوفات (ومن $A_F(V)$) إلى F. إن خواص هذه الدالة تتعلق في معظمها بخواص جمع المصفوفات. الآن نقدم دالة أكثر أهمية وهي معروفة باسم المحددة (determinant) وهي تطبيق من F_n إلى F. إن خواص هذه الدالة تتعلق بخواص ضرب المصفوفات.

بالإضـافـة إلى فاعلية المحددة في برهان بعض المبرهنات فإنها تعتبر مهمة من الناحية «العملية». فإذا كان لدينا مصفوفة T فبإمكاننا باستخدام المحدِّدات أن ننشىء كثيرة حدود معيّنة جذورها هي الجذور المميزة لـ T. وعلاوة على ذلك فإن تكراراي جذر لكثيرة الحدود هذه يقابل تكراره كجذر مميز لـ T. وفي الحقيقة أن كثيرة الحدود المميزة لـ T ، والتي عرفناها سابقا، يمكن أن نحصل عليها عن طريق المحدِّدات.

إن المحـددات تلعب دورًا مهمًا في حل أنظمة المعادلات الخطية. إن هذا هو الاتجاه الذي سنسلكه لبيان أصل المحدِّدات.

إن هناك عدة طرق لتقديم نظرية المحدِّدات بعضها هينٌ ومشوِّق والبعض الآخر ممل وسقيم. وهنا اخترنا طريقة وسطى بين النوعين السابقين، وهي مناسبة لنا لأنها تمكننا من الوصول إلى النتائج التي نحتاجها في دراسة التحويلات الخطية بأسرع ما يمكن.

فيما سيأتي سنعتـبر F حقـلا اختياريا و F_n حلقـة المصفوفات من النوع $n\times n$ على F و $F^{(n)}$ فضـاء المتجهـات الحـاوي على العديدات من نوع n على F. إذا ذكرنا المصفـوفـة فنفهم ضمنًـا أنها عنصر في F_n. كالعـادة سنستعمـل الحـروف الإغريقية للدلالة على عناصر F (إلا إذا ذُكر خلاف ذلك).

لنعتبر نظام المعادلتين

$$\alpha_{11}x_1+\alpha_{12}x_2=\beta_1$$

$$\alpha_{21}x_1+\alpha_{22}x_2=\beta_2$$

ونســأل: تحت أي شروط على α_{ij} يمكننـــا أن نجــد قيم x_1,x_2 لأية قيم لـ β_1,β_2 ؟ بصورة مكافئة إذا كانت لدينا المصفوفة

$$A=\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$$

فمتى تكون A تطبيقا من $F^{(2)}$ على نفسه؟

باستخـدام الـطريقـة التي تعلمناها في المدرسة الثانوية، نحذف x_1 باستعمال المعادلتين، ونجد أن معيار قابلية الحل هو أن $\alpha_{11}\alpha_{22}-\alpha_{12}\alpha_{21}\neq 0$.

الآن نجرب النظام المكون من ثلاث معادلات خطية

$$\alpha_{11}x_1+\alpha_{12}x_2+\alpha_{13}x_3=\beta_1,$$

$$\alpha_{21}x_1+\alpha_{22}x_2+\alpha_{23}x_3=\beta_2,$$
$$\alpha_{31}x_1+\alpha_{32}x_2+\alpha_{33}x_3=\beta_3$$

ومرة أخرى نسأل عن شروط قابلية الحل لقيم اختيارية لـ β_1,β_2,β_3 إذا استخدمنا معادلتين من المعادلات الثلاث فيمكننا حذف x_1 ومن ثم نحذف x_2 من المعادلتين الناتجتين مما يؤدي بنا إلى معيار قابلية الحل وهو كون

$$\alpha_{11}\alpha_{22}\alpha_{33}+\alpha_{12}\alpha_{23}\alpha_{31}+\alpha_{13}\alpha_{21}\alpha_{32}-\alpha_{12}\alpha_{21}a_{33}-\alpha_{11}\alpha_{23}\alpha_{32}-\alpha_{13}\alpha_{22}\alpha_{31}\neq 0$$

بالاستعانة بهذين النموذجين (ومن واقع إدراكنا أن كل شيء سيسير على ما يرام) سوف نقفز قفزة عريضة لنصل إلى الحالة العامة، فنعرف محددة مصفوفة اختيارية من نوع $n\times n$ على F ، ولكن قبل هذا نتعرض لبعض الترميزات.

لتكن S_n زمرة التناظر من الدرجة n. نعتبر أن عناصر S_n تعمل على المجموعة $\{1,2,\ldots,n\}$. لكل عنصر σ في S_n سنعنى بـ $\sigma(i)$ صورة i تحت تأثير σ. (لقد غيرنا ترميزنا هنا فكتبنا التبديل على أنه يعمل من اليسار وليس من اليمين كما كان سابقا. إن السبب وراء ذلك هو تسهيل كتابة الرموز أسفل الحروف. إن الرمز $(-1)^\sigma$ لعنصر σ في S_n سيعني عددا يساوي $+1$ إذا كان التبديل زوجيا و -1 إذا كان البديل فرديا.

تعريف

إذا كانت $A=(\alpha_{ij})$ فإن محددة (determinant) وتُكتب det A هي العنصر $\sum_{\sigma\in S_n}(-1)^\sigma\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)}$ في F.

في بعض الأحيان سنستخدم الرمز

$$\begin{vmatrix} a_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & \alpha_{nn} \end{vmatrix}$$

للدلالة على محددة المصفوفة

$$\begin{pmatrix} a_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & \alpha_{nn} \end{pmatrix}$$

لاحظ أن محددة المصفوفة A هي حاصل جمع (إذا أهملنا الإشارات مؤقتا) لجميع حواصل الضرب الممكنة من العناصر الموجودة داخل A بحيث نأخذ عنصرا واحدا من كل صف وعمود في A. بصورة عامة إن عملية فك محددة مصفوفة هي عملية شائكة ـ حيث إن هناك !n من الحدود في المفكوك ـ ولكن يمكن فك محددة نوع واحد من المصفوفات على الأقل بنظرة واحدة وهذا هو فحوى التمهيدية التالية:

تمهيدية (٦-٩-١)

محددة المصفوفة المثلثة تساوي حاصل ضرب العناصر الموجودة في القطر الرئيسي.

البرهان

هناك حالتان للمصفوفة المثلثة في أولها تكون جميع العناصر الواقعة أعلى القطر الرئيسي مساوية للصفر وفي ثانيها تكون جميع العناصر الواقعة أسفل القطر الرئيسي مساوية للصفر.

نبرهن على النتيجة للمصفوفة A التي على الصيغة

$$\begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ & \alpha_{22} & & \vdots \\ & & \ddots & \vdots \\ & & & \alpha_{nn} \end{pmatrix}$$

وننوه إلى التغيير الواجب إجراؤه على البرهان من أجل النوع الآخر من المصفوفات المثلثة.

لما كان $\alpha_{1i}=0$ عدا الحالة $i=1$ لذا فعند فك محدّدة المصفوفة A نحصل على حدود تساوي الصفر إلا عندما $\sigma(1)=1$. وبناءً على ذلك يكون $\sigma(2)\neq1$ لأن σ تبديل. بيد أنه إذا كان $\sigma(2)<2$ يكون $\alpha_{2\sigma(2)}=0$ وعليه من أجل أن نحصل على حد غير صفري في det A يجب أن يكون $\sigma(2)=2$. بالاستمرار على هذا المنوال يجب أن نحصل على $\sigma(i)=i$ لكل i ، وبناءً على ذلك فإن الحدود غير الصفرية التي تظهر عند فك det (A) هي التي فيها σ هو العنصر المحايد في S_n. لذا فإن حاصل الجمع لـ !n من الحدود يصبح حدًّا واحدًا وهو $\alpha_{11}\alpha_{22}.....\alpha_{nn}$ وهذا ما تنص عليه التمهيدية.

إذا كانت A **مثلثة سفلية** فنبدأ من النهاية المعاكسة فنبرهن على أننا نحصل على حد غير صفري عندما $\sigma(n)=n$ ومن ثم $\sigma(n-1)=n-1$ . . . الخ.

هناك بعض الحالات الشيقة ألا وهي:

١ ـ إذا كانت

$$A=\begin{pmatrix} \lambda_1 & & & & \\ & \lambda_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad \lambda_n \end{pmatrix}$$

مصفوفة قطرية. فإن $\det A=\lambda_1\lambda_2...\lambda_n$.

٢ ـ إذا كانت

$$A=\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad 1 \end{pmatrix}$$

المصفوفة المحايدة فإن $\det A=1$.

٣ ـ إذا كانت

$$A=\begin{pmatrix} \lambda & & & & \\ & \lambda & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad \lambda \end{pmatrix}$$

المصفوفة القياسية، فإن $\det A=\lambda^n$..

لاحظ أيضا إذا كانت جميع عناصر صف (أو عمود) في مصفوفة كلها أصفارًا فإن المحددة تساوي صفرًا لأن كل حد في مفكوك المحدّدة هو حاصل ضرب لعناصر أحدها يساوي صفرًا على الأقل مما يجعل كل حد يساوي صفرًا.

إذا كان $A=(\alpha_{ij})$ في F_n فبإمكاننا اعتبار صفها الأول $v_1=(\alpha_{11},\alpha_{12},\ldots,\alpha_{1n})$ كمتجه في $F^{(n)}$. كذلك بالنسبة لصفها الثاني v_2 وباقي الصفوف. عندئذ يمكننا اعتبار det A دالة لـ n من المتجهات هي $v_1,\ldots,v_n$. يمكن النص على العديد من النتائج بصورة موجزة باستعمال هذه الفكرة، لذا فلنستعمل الترميز $\det A=d(v_1,\ldots,v_n)$ وفي هذا الترميز نعني دائما أن v_1 هو الصف الأول، v_2 الصف الثاني وهكذا، للمصفوفة A.

وملاحظتنا الأخرى هي: بالرغم من أننا نعمل على حقل ولكن بمقدورنا أن نعمل بالسهولة نفسها على حلقة إبدالية فيما عدا بعض المواضع البينة التي نحتاج فيها لعملية تقسيم. سيكون لملاحظتنا هذه أهمية عندما نتكلم لاحقًا في هذا البند عن محدّدات لمصفوفات عناصرها كثيرات حدود.

تمهيدية (٦-٩-٢)

إذا كانت A في F_n و γ في F فإن

$$d(v_1,\ldots,v_{i-1},\gamma v_i,v_{i+1},\ldots,v_n)=\gamma d(v_1,\ldots,v_{i-1},v_i,v_{i+1},\ldots,v_n).$$

لاحظ أن التمهيدية تقول: *إنه إذا ضُربت جميع عناصر صف من صفوف A بعنصر ثابت γ في F فإن محدّدة A نفسها تكون مضروبة بـ γ.*

البرهان

لما كانت عناصر الصف الذي ترتيبه i هي الوحيدة التي غُيِّرت فإن مفكوك $d(v_1,\ldots,v_{i-1},\gamma v_i,v_{i+1},\ldots,v_n)$ يصبح

$$\sum_{\sigma\in S_n}(-1)^\sigma\alpha_{1\sigma(1)}\cdots\alpha_{i-1,\sigma(i-1)}(\gamma\alpha_{i\sigma(i)})\alpha_{i+1,\sigma(i+1)}\cdots\alpha_{n\sigma(n)}$$

وحيث إن هذا يساوي

$$\gamma\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\alpha_{i,\sigma(i)}\cdots\alpha_{n\sigma(n)}$$

وهذا بدوره يساوي

$$\gamma d(v_1,\ldots,v_n)$$

تمهيدية (٦-٩-٣)

$$d(v_1,\ldots,v_{i-1},v_i,v_{i+1},\ldots,v_n)+d(v_1,\ldots,v_{i-1},u_i,v_{i+1},\ldots,v_n)=d(v_1,\ldots,v_{i-1},v_i+u_i,v_{i+1},\ldots,v_n)$$

قبل برهان هذه النتيجة دعنا ننظر لما تعنيه وما لا تعنيه. **إنها لا تعني أن** $\det A+\det B=\det(A+B)$ حيث إن هذا خطأ يمكن اكتشافه من خلال المثال التالي:

$$A=\begin{pmatrix}1&0\\0&0\end{pmatrix},\ B=\begin{pmatrix}0&0\\0&1\end{pmatrix}$$

إذ أن $\det A=\det B=0$ بينما $\det(A+B)=1$. إن ما تعنيه التمهيدية هو أنه إذا كانت A و B مصفوفتين متساويتين لجميع الصفوف ما عدا الصف الذي ترتيبه i فإن محددة المصفوفة المكونة من A و B باستخدام جميع صفوف A عدا الصف الذي ترتيبه i والذي نحصل عليه من جمع الصفين اللذين ترتيبهما i من A و B على الترتيب، محددة هذه المصفوفة تساوي $\det A+\det B$. إذا كانت

$$A=\begin{pmatrix}1&2\\3&4\end{pmatrix},\ B=\begin{pmatrix}1&1\\3&4\end{pmatrix}$$

فإن $\det A=-2$ و $\det B=1$ ، $\det\begin{pmatrix}2&3\\3&4\end{pmatrix}=-1=\det A+\det B$.

برهان التمهيدية

إذا كان $v_1=(\alpha_{11},\ldots,\alpha_{1n})$ ، . . . ، $v_i=(\alpha_{i1},\ldots,\alpha_{in})$ ، . . . ، $v_n=(\alpha_{n1},\ldots,\alpha_{nn})$ وكان $u_i=(\beta_{i1},\ldots,\beta_{in})$ ، فإن

$$d(v_1,\ldots,v_{i-1},u_i+v_i,v_{i+1},\ldots,v_n)$$
$$=\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\ \alpha_{i-1,\sigma(i-1)}(\alpha_{i\sigma(i)}+\beta_{i\sigma(i)})\alpha_{i+1,\sigma(i+1)}\cdots\ \alpha_{n\sigma(n)}$$
$$=\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\ \alpha_{i-1,\sigma(i-1)}\alpha_{i\sigma(i)}\cdots\alpha_{n\sigma(n)}$$
$$+\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\alpha_{i-1,\sigma(i-1)}\beta_{i\sigma(i)}\cdots\alpha_{n\sigma(n)}$$
$$=d(v_1,\ldots,v_i,\ldots,v_n)+d(v_1,\ldots,u_i,\ldots v_n)$$

إن الخصـائص المضمنـة في التمهيديات (٦-٩-١)، (٦-٩-٢) و(٦-٩-٣) بالإضافة إلى ما تنص عليه التمهيدية القادمة تميز دالة المحددة (انظر مسألة ١٣ في نهاية هذا البند). لذا فإن الخاصة الشكلية التي تعرضها التمهيدية القادمة تعتبر أساسية في نظرية المحددات.

تمهيدية (٦-٩-٤)

إذا تساوى صفين من صفوف A (أي $v_r=v_s$ ، $r\neq s$) فإن $\det A=0$.

البرهان

لتكن $A=(\alpha_{ij})$ ولنفرض أنه لـ r و s حيث $r\neq s$ يكون $\alpha_{rj}=\alpha_{sj}$ لكل j.
لنعتبر المفكوك

$$\det A=\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\ \alpha_{r\sigma(r)}\cdots\alpha_{s\sigma(s)}\cdots\alpha_{n\sigma(n)}$$

في هذا المفكـوك نقرن الحدود كالتالي: لـ σ في S_n نقرن الحد $(-1)^{\sigma}\alpha_{1\sigma(1)}\ldots\alpha_{n\sigma(n)}$ مع الحـد $(-1)^{\tau\sigma}\alpha_{1\tau\sigma(1)}\ldots\alpha_{n\tau\sigma(n)}$ حيث τ هو المنـاقلة $(\sigma(r),\sigma(s))$. ولمـا كان τ مناقلة، فإن $\tau^2=1$. إن هذا حقـا يعـطينـا اقترانًا. ولكن $\alpha_{r\sigma(r)}=\alpha_{s\sigma(r)}$ بالفرض و $\alpha_{r\sigma(r)}=d_{s\tau\sigma(s)}$ فنحصل على $\alpha_{r\sigma(r)}=\ \alpha_{s\tau\sigma(s)}$. وبصورة مشابهة نحصل على $\alpha_{s\sigma(s)}=\alpha_{r\tau\sigma(r)}$. ومن ناحية أخرى $\tau\sigma(i)=\sigma(i)$ و $\alpha_{i\sigma(i)}=\alpha_{i\tau\sigma(i)}$ لكل $i\neq r$ و $i\neq s$. لذا فإن الحدين $\alpha_{i\sigma(1)}\ldots\alpha_{n\sigma(n)}$ و $\alpha_{1\tau\sigma(1)}\ldots\alpha_{n\tau\sigma(n)}$ متساويان إن إشارة الحد الأول $(-1)^{\sigma}$ بينما إشارة الحد الثاني $(-1)^{\tau\sigma}$ في مفكوك $\det A$. لما كان τ مناقلة وهو تبديل فردي

لذا يكون $(-1)^{\tau\sigma}=-(-1)^{\sigma}$. إذن في عملية اقتران الحدود يلغي الحدين المقترنين ببعضهما في حاصل الجمع مما يجعل $\det A=0$. (إن البرهان لا يعتمد على مميز F ويبقى صحيحًا حتى في حالة كون مميز F يساوي 2).

من النتائج التي حصلنا عليها حتى الآن يمكننا تحديد تأثير مبادلة صفوف مصفوفة على قيمة محدِّدتها.

تمهيدية (٦-٩-٥)

إن مبادلة صفين في A يغير إشارة محددتها.

البرهان

نظرا لتساوي صفين فإن المحدِّدة:

$$d(v_1,\dots,v_{i-1},v_i+v_j,v_{i+1},\dots,v_{j-1},v_i+v_j,v_{j+1},\dots,v_n)=0$$

وذلك وفقا لتمهيدية (٦-٩-٤). باستخدام تمهيدية (٦-٩-٣) عدة مرات نحصل على:

$$d(v_1,\dots,v_{i-1},v_i,\dots,v_{j-1},v_j,\dots,v_n)+\ d(v_1,\dots,v_{i-1},v_j,\dots,v_{j-1},v_i,\dots,v_n)+$$
$$d(v_1,\dots,v_{i-1},v_i,\dots,v_{j-1},v_i,\dots,v_n)+d(v_1,\dots,v_{i-1},v_j,\dots,v_{j-1},v_j,\dots,v_n)=0$$

ولكن في كلا الحدين الأخيرين يوجد صفان متساويان مما يجعل محدّدة كل منهما تساوي صفرًا حسب تمهيدية (٦-٩-٤). لذا فإن العلاقة أعلاه تصبح:

$$d(v_1,\dots,v_{i-1},v_i,\dots,v_{j-1},v_j,\dots,v_n)+\ d(v_1,\dots,v_{i-1},v_j,\dots,v_{j-1},v_i,\dots,v_n)=0$$

وهذا ما تنص عليه التمهيدية.

نتيجـــة

إذا كانت B مصفوفة نحصل عليها من المصفوفة A بتبديل لمواقع صفوفها فإن $\det A=\pm\det B$ حيث إن الإشارة 1+ إذا كان التبديل زوجيًا و 1- إذا كان التبديل فرديًا.

الآن نحن في وضع يمكّننا من الاستفادة مما سبق لبرهان الخاصة الجبرية الأساسية لدالّة المحدّدة وهي خاصة حفظ حاصل الضرب. وبهذا يكون للمحدّدة ميزات تحصل عليها من كونها تشاكل من البناء الضربي لـ F_n إلى F.

مبرهنة (٦-٩-١)

إذا كانت A و B في F_n فإن $det\,(AB)=det\,(A)\,det\,(B)$.

البرهان

لتكن $A=(\alpha_{ij})$ و $B=(\beta_{ij})$ ولتكن صفوف B هي المتجهات $u_1,u_2,\ldots,u_n$. نعرِّف n من المتجهات كما يلي:

$$w_1=\alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n$$

$$w_2=\alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n$$

$$\vdots$$

$$w_n=\alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n$$

ولنعتبر $d(w_1,\ldots,w_n)$. بفك هذه المحددة وبالاستعانة عدة مرات بالتمهيديتين (٦-٩-٢) و(٦-٩-٣) نحصل على:

$$d(w_1,\ldots,w_n)=\sum_{i_1,i_2,\ldots,i_n}\alpha_{1i_1}\alpha_{2i_2}\ldots\,\alpha_{ni_n}d(u_{i_1},u_{i_2},\ldots,u_{i_n})$$

في حاصل الجمع المتعدد هذا، تتغير المقادير $i_1,\ldots,i_n$ بصورة مستقلة عن بعضها من 1 إلى n. ولكن إذا كان $i_r=i_s$ فإن $u_{i_r}=u_{i_s}$ مما يجعل $d(u_{i_1},\ldots,u_{i_r},\ldots,u_{i_s},\ldots,u_{i_n})=0$ وفقا لتمهيدية (٦-٩-٤). وبعبارة أخرى إن الحدود الوحيدة في حاصل الجمع والتي يمكن أن تعطينا مقدارًا غير صفري هي الحدود التي فيها تكون $i_1,i_2,\ldots,i_n$ مختلفة، أي التي يكون بها التطبيق

$$\sigma=\begin{pmatrix}1 & 2 & \ldots & n\\ i_1 & i_2 & \ldots & i_n\end{pmatrix}$$

تبديل لـ $1,2,\ldots,n$. وأيضا كل تبديل من هذا النوع ممكن حدوثه. أخيرا لاحظ أنه وفقًا لنتيجة تمهيدية (٦-٩-٥) تكون:

$$d(u_{i_1},u_{i_2},\ldots,u_{i_n})=(-1)^{\sigma}d(u_1,u_2,\ldots,u_n)\ =(-1)^{\sigma}\det B$$

حيث σ هو التبديل $\begin{pmatrix}1 & 2 & \ldots & n\\ i_1 & i_2 & \ldots & i_n\end{pmatrix}$.

لذا نحصل على

$$d(w_1,\ldots,w_n)=\sum_{\sigma\in S_n}\alpha_{1\sigma(1)}\ldots\alpha_{n\sigma(n)}(-1)^{\sigma}\det B$$

$$d(w_1,\ldots,w_n)=\det A\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\ldots\alpha_{n\sigma(n)}$$

$$d(w_1,\ldots,w_n)=(\det B)\ (\det A)$$

الآن نود أن نثبت أن $d\ (w_1,\ldots,W_n)$ تساوي $\det(AB)$. ولكن، لما كان

$$w_1=\alpha_{11}u_1+\ldots+\alpha_{1n}u_{1n},w_2=\alpha_{21}u_1+\ldots+\ \alpha_{2n}u_n,\ldots,w_n=\alpha_{n1}u_1+\ldots+\alpha_{nn}u_n$$

فإننا نحصل على أن $d(w_1,\ldots,w_n)$ هي $\det C$ حيث إن الصف الأول في C هو w_1 والثاني هو w_2 الخ.

بيد أنه إذا كتبنا w_1 بدلالة الإحداثيات نحصل على:

$$w_1=\alpha_{11}u_1+\ldots+\alpha_{1n}u_n=\alpha_{11}(\beta_{11},\beta_{12},\ldots,\beta_{1n})+\ldots+\alpha_{1n}(\beta_{n1},\ldots,\beta_{nn})$$

$$=(\alpha_{11}\beta_{11}+\alpha_{12}\beta_{21}+\ldots+\alpha_{1n}\beta_{1n},\alpha_{11}\beta_{12}+\ \ldots+\alpha_{1n}\beta_{n2},\ldots,\alpha_{11}\beta_{1n}+\ldots+\alpha_{1n}\beta_{nn})=$$

وهذا هو الصف الأول في AB. وبصورة مشابهة w_2 هو الصف الثاني في AB وهكذا بالنسبة لباقي الصفوف. لذا نحصل على $C=AB$ وحيث إن

$$\det(AB)=\det C=d(w_1,\ldots,w_n)=(\det A)\ (\det B)$$

نكون قد أنهينا برهان المبرهنة.

نتيجــة (١)

إذا كان لـ A معكوس فإن $\det A\neq 0$ و $\det(A^{-1})=(\det A)^{-1}$

البرهان

لما كان $AA^{-1}=1$ فإن $\det(AA^{-1})=\det 1=1$. لذا فباستخدام المبرهنة نحصل على $1=\det(AA^{-1})=(\det A)\ (\det A^{-1})$. إن هذه العلاقة تنص على أن $\det A\neq 0$ وأن $\det A^{-1}=1/\det A$.

نتيجـــة (٢)

إذا كان لـ A معكوس فإنه لكل مصفوفة B تكون $\det(ABA^{-1})=\det B$

البرهان

باستخدام المبرهنة في حالة $(AB)A^{-1}$ ، نحصل على

$$\det((AB)A^{-1})=\det(AB)\det(A^{-1})=\det A \det B \det(A^{-1})$$

وباستعمال نتيجة (١) يمكننا تبسيط الطرف الأخير إلى $\det B$. لذا تكون

$$\det(ABA^{-1})=\det B$$

إن النتيجة (٢) تمكننا من تعريف محدّدة التحويل الخطي . ولأجل ذلك دع T في $A(V)$ و $m_1(T)$ مصفوفة T بالنسبة إلى أساس في V. إذا كان لدينا أساس آخر لـ V وكانت $m_2(T)$ مصفوفة T بالنسبة لهذا الأساس فإنه وفقًا لمبرهنة (٦-٣-٢)، $m_2(T)=Cm_1(T)C^{-1}$ وعليه $\det(m_2(T))=\det(m_1(T))$ وفقا للنتيجة (٢) أعلاه . أي محدّدة مصفوفة T بالنسبة لأي أساس لا تتغير بتغيير الأساس. لذا فإن التعريف: *$\det T=\det m_1(T)$ هي في الحقيقية لا تعتمد على الأساس وتعرف بدالّة المحدّدة على $A(V)$.*

في إحدى المسائل الماضية كانت غاية المسألة هي برهان أن A'، منقول المصفوفة A (transpose)، تشابه المصفوفة A . وبفرضنا صحة تلك المسألة (والتي هي كذلك) نحصل على أن $\det(A')=\det(A)$ حسب نتيجة (٢) أعلاه . لذا فإنه ليس من المستغرب أن نقدم هنا برهانًا مباشرًا لهذه الحقيقية .

تمهيدية (٦-٩-٦)

$$\det A=\det A'$$

البرهان

لتكن $A=(\alpha_{ij})$ و $A'=(\beta_{ij})$ ومن المؤكد أن $\beta_{ij}=\alpha_{ji}$. الآن

$$\det A=\sum_{\sigma\in S_n}(-1)^{\sigma}\alpha_{1\sigma(1)}\cdots\alpha_{n\sigma(n)}$$

بينما

$$\det A' = \sum_{\sigma \in S_n} (-1)^\sigma \beta_{1\sigma(1)} \dots \beta_{n\sigma(n)} = \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}$$

ولكن الحد $(-1)^\sigma \alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}$ يساوي $(-1)^\sigma \alpha_{1\sigma^{-1}(1)} \dots \alpha_{n\sigma^{-1}(1)}$ (برهن ذلك). وحيث إن $(-1)^\sigma = (-1)^{\sigma^{-1}}$ أي أنه إذا كان σ فرديًا فإن σ^{-1} فردي بينما إذا كان σ زوجيًا فإن σ^{-1} زوجي. وعليه نحصل على

$$(-1)^\sigma \alpha_{1\sigma^{-1}(1)} \dots \alpha_{n\sigma^{-1}(n)} = (-1)^{\sigma^{-1}} \alpha_{1\sigma^{-1}(1)} \dots \alpha_{n\sigma^{-1}(n)}$$

وأخيرا لاحظ إذا تغيرت σ في مجال S_n فكذلك الحال بالنسبة لـ σ^{-1} لذا.

$$\det A' = \sum_{\sigma \in S_n} (-1)^{\sigma^{-1}} \alpha_{1\sigma^{-1}(1)} \dots \alpha_{n\sigma^{-1}(n)}$$

$$\det A' = \sum_{\sigma \in S_n} (-1)^\sigma \alpha_{1\sigma(1)} \dots \alpha_{n\sigma(n)} = \det A$$

على ضوء تمهيدية (٦-٩-٦) نرى أن عملية تبادل صفوف وأعمدة مصفوفة لا يغير قيمة محدِّدتها. نستنتج من ذلك *التمهيديات (٦-٩-٢) إلى (٦-٩-٥) التي عنت بعمليات على صفوف المصفوفة تبقى صحيحة بالنسبة لذات العمليات على أعمدتها.*

تستعمل هذه الملاحظة لاشتقاق قاعدة كريمر (Cramer's rule) لحل نظام المعادلات الخطية.

إذا كان لدينا نظام معادلات خطيّة

$$\begin{aligned} &\alpha_{11}x_1 + \dots + \alpha_{1n}x_n = \beta_1 \\ &\vdots \\ &\alpha_{n1}x_1 + \dots + \alpha_{nn}x_n = \beta_n \end{aligned}$$

ندعو $A = (\alpha_{ij})$ بمصفوفة النظام و $\triangle = \det A$ *بمحدّدة النظام* نفرض أن $\Delta \neq 0$ ، أي

$$\triangle = \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \\ \alpha_{n1} & \dots & \alpha_{nn} \end{vmatrix} \neq 0$$

وفقا لتمهيدية (٦-٩-٢) (في حالة الأعمدة بدلاً من الصفوف) يكون

$$x_i\triangle=\begin{vmatrix}\alpha_{11}\ \dots\ \alpha_{1i}x_i\ \dots\ \alpha_{1n}\\ \vdots\\ \alpha_{n1}\ \dots\ \alpha_{ni}x_i\ \dots\ \alpha_{nn}\end{vmatrix}$$

ولكن كنتيجة للتمهيديتين (٦-٩-٣) و(٦-٩-٤) يمكن جمع أي مضاعف لعمود مع آخر دون تغيير المحدّدة (انظر مسألة ٥). اجمع مع العمود الذي ترتيبه i في $x_i\triangle$ كلا من x_1 ضرب العمود الأول وx_2 ضرب العمود الثاني و. . . وx_j ضرب العمود الذي ترتيبه j $(j\neq i)$ ، فنحصل على

$$x_i\triangle=\begin{vmatrix}\alpha_{11}\dots\alpha_{1,i-1} & (\alpha_{11}x_1+\alpha_{12}x_2+\dots+\alpha_{1n}x_n) & \alpha_{1,i+1}\dots\alpha_{1n}\\ \vdots & \vdots & \vdots\\ \alpha_{n1}\dots\alpha_{n,i-1} & (\alpha_{n1}x_1+\alpha_{n2}x_2+\dots+\alpha_{nn}x_n) & \alpha_{n,i+1}\dots\alpha_{nn}\end{vmatrix}$$

وباستعمال

$$\alpha_{k1}x_1+\dots+\alpha_{kn}x_n=\beta_k$$

نحصل أخيرا على:

$$x_i\triangle=\begin{vmatrix}\alpha_{11}\dots\alpha_{1,i-1} & \beta_1 & \alpha_{1,i+1} & \dots\alpha_{1n}\\ \cdot & \cdot & \cdot & \cdot\\ \alpha_{n1}\dots\alpha_{n,i-1} & \beta_n & \alpha_{1,i+1} & \dots\alpha_{nn}\end{vmatrix}$$

حيث نرمز للطرف الأيمن بـ $\triangle_i$. إذن $x_i=\triangle_i/\triangle$. أي أننا نحصل على المبرهنة التالية.

مبرهنة (٦-٩-٢) *(قاعدة كريمر Cramer's rule)*

إذا كانت $\triangle$ محدّدة نظام المعادلات الخطية.

$$\alpha_{11}x_1+\dots+\alpha_{1n}x_n=\beta_1$$
$$\vdots$$
$$\alpha_{n1}x_1+\dots+\alpha_{nn}x_n=\beta_n$$

وكانت $\triangle\neq0$ فإن حل النظام يعطى بالقاعدة $x_i=\triangle_i/\triangle$ حيث $\triangle_i$ هي المحدّدة التي نحصل عليها من $\triangle$ بوضع $\beta_1,\beta_2,\dots,\beta_n$ بدلا من العمود الذي ترتيبه i في $\triangle_i$.

مثال على ذلك اعتبر النظام

$$x_1+2x_2+3x_3=-5$$
$$2x_1+x_2+x_3=-7$$
$$x_1+x_2+x_3=0$$

إن محددته

$$\Delta=\begin{vmatrix}1 & 2 & 3\\ 2 & 1 & 1\\ 1 & 1 & 1\end{vmatrix}=1\neq 0$$

وعليه

$$x_1=\frac{\begin{vmatrix}-5 & 2 & 3\\ -7 & 1 & 1\\ 0 & 1 & 1\end{vmatrix}}{\Delta}\ ,\ x_2=\frac{\begin{vmatrix}1 & -5 & 3\\ 2 & -7 & 1\\ 1 & 0 & 1\end{vmatrix}}{\Delta}\ ,\ x_3=\frac{\begin{vmatrix}1 & 2 & -5\\ 2 & 1 & -7\\ 1 & 1 & 0\end{vmatrix}}{\Delta}$$

يمكننا إيجاد صلة بين إمكانية وجود معكوس ضربي لمصفوفة (أو تحويل خطي) مع قيمة المحدّدة لها، أي أن المحدّدة تعطينا معيارًا لذلك.

مبرهنة (٦-٩-٣)

يوجد لـ A معكوس إذا وفقط إذا كانت $\det A\neq 0$

البرهان

إذا كان لـ A معكوس فقد رأينا من نتيجة (١) لمبرهنة (٦-٩-١) أن $\det A\neq 0$.
من ناحية أخرى لنفرض أن $\det A\neq 0$ حيث $A=(\alpha_{ij})$. باستخدام قاعدة كريمر يمكننا حل النظام.

$$\begin{matrix}\alpha_{11}x_1+\ldots+\alpha_{1n}x_n=\beta_1\\ \vdots \qquad\qquad \vdots\\ \alpha_{n1}x_1+\ldots+\alpha_{nn}x_n=\beta_n\end{matrix}$$

في المجاهيل $x_1,\dots,x_n$ لأي قيم اختيارية لـ $\beta_1,\dots,\beta_n$. لذا فإن A باعتبارها تحويلاً خطيًا على $F^{(n)}$ هي تطبيق غامر. وفي الحقيقة أن المتجه $(\beta_1,\dots,\beta_n)$ هو صورة $(\frac{\Delta_1}{\Delta},\dots,\frac{\Delta_n}{\Delta})$ تحت تأثير A'. ولكون A' غامرا فوفقا لمبرهنة (٦-١-٤) يوجد معكوس لـ A' وبناء عليه يوجد معكوس لـ A (برهن على ذلك).

يمكننا النظر إلى مبرهنة (٦-٩-٣) من زاوية أخرى قد تكون أكثر تشويقًا. إذا كانت A في F_n فيمكننا إدخالها في K_n حيث K امتداد لـ F نختاره بحيث يمكننا تحويل A في K_n إلى صيغة مثلثة وعليه توجد B في K_n بحيث أن:

$$BAB^{-1}=\begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ & \lambda_2 & & \cdot \\ * & & \cdot & \cdot \\ & & \cdot & \lambda_n \end{pmatrix}$$

حيث $\lambda_1,\dots,\lambda_n$ هي جميع الجذور المميزة لـ A مذكورة هنا حسب تكرارها كجذور لكثير الحدود المميز لـ A. لذا فإن

$$\det A=\det(BAB^{-1})=\lambda_1\lambda_2\dots\lambda_n$$

وفقا لتمهيدية (٦-٩-١). ولكن A لها معكوس إذا وفقط إذا لم تكن أي من جذورها المميزة يساوي صفرًا. ولكن $\det A\neq 0$ إذا وفقط إذا كان $\lambda_1,\lambda_2\dots\lambda_n\neq 0$ أي إذا لم يكن أي من جذورها المميزة يساوي صفرًا. لذا فإن لـ A معكوس إذا وفقط إذا كانت $\det A\neq 0$.

إن للبرهان البديل المقدم أعلاه بعض المزايا حيث إننا بإنجازه برهنا نتيجة جزئية مشوقة بحد ذاتها، ألا وهي.

تمهيدية (٦-٩-٧)

إن $\det A$ هي حاصل ضرب الجذور المميزة لـ A آخذين بنظر الاعتبار تكرار هذه الجذور.

تعريف

إذا كانت A في F_n فإن ***المعادلة العامة*** *(secular equation) لـ A هي كثيرة الحدود det (x–A) في F[x].*

إن ما أطلقنا عليه المعادلة العامة لـ A يسمى عادة بكثيرة الحدود المميزة لـ A. ولكننا سبق وأن عرّفنا كثيرة الحدود المميزة لـ A بأنه حاصل ضرب القواسم الابتدائية لـ A. في الحقيقة (انظر مسألة ٨) إن كثيرة الحدود المميزة لـ A تساوي المعادلة العامة، ولكن لأننا لم نرد تطوير هذا المفهوم بصورة صريحة أثناء الشرح استعملنا تعبير المعادلة العامة.

دعنا نحسب المثال التالي، إذا كانت

$$A=\begin{pmatrix}3 & 0\\ 1 & 2\end{pmatrix}$$

فإن

$$x-A=\begin{pmatrix}x & 0\\ 0 & x\end{pmatrix}-\begin{pmatrix}1 & 2\\ 3 & 0\end{pmatrix}=\begin{pmatrix}x-1 & -2\\ -3 & x\end{pmatrix}$$

وعليه فإن

$$\det (x-A)=(x-1)x-(-2)(-3)=x^2-x-6$$

فتكون المعادلة العامة للمصفوفة

$$\begin{pmatrix}1 & 2\\ 3 & 0\end{pmatrix}$$

هي x^2-x-6.

هناك بعض الملاحظات المتعلقة بالمعادلة العامة: إذا كان λ جذرا لـ det (x–A) فإن det (λ–A)=0. لذا لا يوجد معكوس لـ λ–A حسب مبرهنة (٦ـ٩ـ٣) وهذا يجعل λ جذرًا مميزًا لـ A. وبالعكس إذا كان λ جذرًا مميزًا لـ A فلا يوجد معكوس لـ λ–A مما يجعل det (λ–A)=0 وعليه يكون λ جذرًا لـ det (x–A). لذا فإن جذور كثيرة الحدود التي يمكن حسابها بصورة صريحة والتي أطلقنا عليها اسم المعادلة العامة هي بالضبط الجذور المميزة لـ A. إننا نريد أن نخطو خطوة أخرى في هذا المجال فنبين أن تكرار أي جذر في المعادلة العامة هو بالضبط نفس تكراره كجذر مميز لـ A. فإذا كان λ_i جذرًا

مميزًا لـ A تكراره m_i فإنه يمكننا كتابة A بالصيغة المثلثة كما هو موضح في شكل (٦-٩-١) حيث λ_i يظهر في القطر m_i من المرات

$$BAB^{-1} = \begin{pmatrix} \lambda_1 & & & & 0 & \cdots & & 0 \\ & \ddots & & & & & & \\ & & \lambda_1 & & & & & \\ & & & \lambda_2 & & & & \\ & & & & \ddots & & & \\ & & & & & \lambda_2 & & \vdots \\ & & * & & & & \lambda_k & 0 \\ & & & & & & & \ddots \\ & & & & & & & \lambda_k \end{pmatrix}$$

شكل (٦-٩-١)

ولكن كما هو موضح بالمصفوفة في شكل (٦-٩-٢) فإن

$$\det(x-A) = \det(B(x-A)B^{-1}) = (x-\lambda_1)^{m_1}(x-\lambda_2)^{m_2}\ldots(x-\lambda_k)^{m_k}$$

ولهذا فإن

$$B(x-A)B^{-1} = x - BAB^{-1} =$$

$$\begin{pmatrix} x-\lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & x-\lambda_1 & & & & \\ & & & x-\lambda_2 & & & \\ & & & & \ddots & & \\ & & & & & x-\lambda_2 & \\ & * & & & & & x-\lambda_k \\ & & & & & & & \ddots \\ & & & & & & & & x-\lambda_k \end{pmatrix}$$

شكل (٦-٩-٢)

وعليه فإن كل λ_i الذي تكراره يساوي m_i كجذر مميز لـ A هو جذر لكثيرة الحدود det (x–A) تكرارها يساوي m_i أيضا. بهذا نكون قد برهنا ما يلي.

مبرهنة (٦-٩-٤)

إن الجذور المميزة لـ A بتكرارها الصحيح هي جذور المعادلة العامة det (x-A).

نهي هذا البند بمبرهنة كيلي ـ هاملتون (Cayley-Hamilton) التاريخية المهمة.

مبرهنة (٦-٩-٥)

كل مصفوفة A في F_n تحقق معادلتها العامة .

البرهان

في K_n إذا كان لدينا مصفوفة B لها معكوس، حيث K أي امتداد لـ F فإن A و BAB^{-1} يحققان نفس كثيرات الحدود. كذلك لما كانت

$$\det(x-BAB^{-1})=\det(B(x-A)B^{-1})=\det(x-A)$$

فإن A, BAB^{-1} لهما المعادلة العامة نفسها. إذا أمكننا بيان أن BAB^{-1} تحقق معادلتها العامة فسينتج عن هذا أن A كذلك. ولكننا يمكن أن نختار $B, K\supset F$ في K_n بحيث أن BAB^{-1} مصفوفة مثلثة ولقد رأينا سابقا (مبرهنة ٦-٤-٢) إن المصفوفة المثلثة تحقق معادلتها العامة، إن هذا ينهي برهان المبرهنة.

مسائل

١ - إذا كان F حقل الأعداد المركبة، فجد قيمة المحدِّدات التالية

(ا) $\begin{vmatrix} 1 & i \\ 2-i & 3 \end{vmatrix}$ ، (ب) $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$ ، (جـ) $\begin{vmatrix} 5 & 6 & 8 & -1 \\ 4 & 3 & 0 & 0 \\ 10 & 12 & 16 & -2 \\ 1 & 2 & 3 & 4 \end{vmatrix}$

٢ - لأي مميز للحقل F تكون المحدّدتان التاليتان مساويتين للصفر.

(ا) $\begin{vmatrix} 1 & 2 & 3 & 0 \\ 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 4 & 5 & 6 \end{vmatrix}$ ؟ (ب) $\begin{vmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \\ 5 & 3 & 4 \end{vmatrix}$ ؟

٣ - إذا كانت A مصفوفة عناصرها أعداد صحيحة وكانت A^{-1} مصفوفة عناصرها أعداد صحيحة أيضا فماذا يمكن أن تكون قيمة محدّدة A ؟

٤ ـ أثبت أن إضافة مضاعف لصف إلى صف آخر لا يغير قيمة محدّدة المصفوفة.

*٥ ـ إذا كانت لدينا المصفوفة $A=(\alpha_{ij})$ وكانت A_{ij} المصفوفة التي نحصل عليها من A بحـذف الصف الذي ترتيبه i و العمود الذي ترتيبه j. دع $M_{ij}=(-1)^{i+j}\det A_{ij}$. يسمى M_{ij} العامل المرافق لـ α_{ij}. برهن على أن $\det A=\alpha_{i1}M_{i1}+\ldots+\alpha_{in}M_{in}$.

٦ ـ (ا) إذا كانت A و B مصفوفتين جزئيتين مربعتين. برهن على أن

$$\det\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}=(\det A)\,(\det B)$$

(ب) عمم الجزء (ا) إلى

$$\det\begin{pmatrix} A_1 & & & & * \\ & A_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & A_n \end{pmatrix}$$

حيث A_i *مصفوفات جزئية مربعة.*

٧ ـ إذا كانت $C(f)$ المصفوفة المصاحبة لكثيرة الحدود $f(x)$. فبرهن على أن المعادلة العامة لـ $C(f)$ هي $f(x)$.

٨ ـ باستعمال المسألتين ٦ و٧. أثبت أن المعادلة العامة لـ A هي كثيرة الحدود المميزة لـ A. (انظر بند (٦ـ٧)، إن هذا يبرهن على الملاحظة المذكورة سابقا والقائلة بأن جذور $p_T(x)$ هي نفس الجذور المميزة لـ T وبالتكرار نفسه).

٩ ـ باستعمال مسألة (٨). أعط برهانا بديلا لمبرهنة كيلي هاملتون.

١٠ ـ إذا كان F حقـل الأعداد النسبية. فاحسب المعادلة العامة، الجذور المميزة، وتكرار هذه الجذور لكل من

(ا) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$، (ب) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 7 \end{pmatrix}$، (جـ) $\begin{pmatrix} 4 & 1 & 1 & 1 \\ 1 & 4 & 1 & 1 \\ 1 & 1 & 4 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix}$

١١ ـ لكل من المصفوفات المذكورة في مسألة (١٠) تأكد من أن أيًّا منها تحقق معادلتها العامة وذلك باستخدام الطرق المباشرة في حساب المصفوفات.

*١٢ ـ إذا كانت مرتبة A تساوي r. فبرهن على أنه توجد مصفوفة جزئية من نوع $r\times r$ في المصفوفة A بحيث أن محدِّدتها لا تساوي صفرًا، وإذا كان $r<n$ فلا توجد مصفوفة جزئية من نوع $(r+1)\times(r+1)$ في A تتمتع بهذه الخاصة.

*١٣ ـ لتكن f دالة في n من المتغيرات من $F^{(n)}$ إلى F بحيث

(ا) $f(v_1,\ldots,v_n)=0$ إذا كان $v_i=v_j$ في $F^{(n)}$ و $i\neq j$.

(ب) $f(v_1,\ldots,\alpha v_i,\ldots,v_n)=\alpha f(v_1,\ldots,v_i,\ldots,v_n)$ لكل i ولكل α في F.

(جـ) $f(v_1,\ldots,v_i+u_i,\ldots,v_n)=f(v_1,\ldots,v_i,\ldots,v_n)+f(v_1,\ldots,u_i,\ldots,v_n)$

(د) $f(e_1,\ldots,e_n)=1$ حيث $e_1=(1,0,\ldots,0)$ ، $e_2=(0,1,0,\ldots,0)$ ، . . . ، $e_n=(0,0,\ldots,0,1)$

برهن على أن $f(v_1,\ldots,v_n)=\det A$ لكل $A\in F_n$ حيث v_1 هو الصف الأول في A ، v_2 الصف الثاني . . . الخ.

١٤ ـ استخدم مسألة (١٣) كي تبرهن على أن $\det A'=\det A$

١٥ ـ (ا) برهن على أن لـ AB و BA المعادلة العامة (المميزة) نفسها.

(ب) أعط مثالاً تكون فيه كثيرة الحدود الدنيا لـ AB مختلفة عن كثيرة الحدود الدنيا لـ BA.

١٦ ـ إذا كانت A مثلثة. فأثبت باستخدام حسابات مباشرة أن A تحقق معادلتها العامة.

١٧ ـ استخدام قاعدة كريمر لإيجاد الحلول في حقل الأعداد الحقيقية للنظامين

(ا)
$$x+y+z=1$$
$$2x+3y+4z=1,$$
$$x-y-z=0$$

(ب)
$$x+y+z+w=1$$
$$x+2y+3z+4w=0$$
$$x+y+4z+5w=1$$
$$x+y+5z+6w=0$$

١٨ ـ (ا) لتكن $GL(n,F)$ مجموعة كل المصفوفات في F_n التي محدِّدتها لا تساوي صفرًا. برهن على أن $GL(n,F)$ زمرة بالنسبة لعملية ضرب المصفوفات.

(ب) لتكن $D(n,F)=\{A\in GL(n,F) | \det A=1\}$. برهن على أن $D(n,F)$ زمـــرة جزئية ناظمية في $GL(n,F)$.

(جـ) أثبت أن $GL(n,F)/D(n,F)$ تماثل زمرة العناصر غير الصفرية في F بالنسبة لعملية الضرب.

١٩ ـ إذا كان K امتدادا للحقل F وجعلنا $E(n,K,F)=\{A\in GL(n,K) | \det A\in F\}$

(ا) برهن على أن $E(n,K,F)$ زمرة جزئية ناظمية في $GL(n,K)$

(ب)* عيّن $GL(n,K)/E(n,K,F)$.

٢٠*ـ إذا كان F حقل الأعداد النسبية. فبرهن على أنه إذا كانت N زمرة جزئية ناظمية في $D(2,F)$ فإنه إما $N=D(2,F)$ أو أن N تحتوي على مصفوفات قياسية فقط.

(٦-١٠) التحويلات الهرميتية، الواحدية والناظمية

من خلال دراستنا السابقة للتحويلات الخطية وجدنا أن الطبيعة الخاصة للحقل F تلعب دورا مهما نسبيا. ويتضح لنا هذا عادة فيما يتعلق بالجذور المميزة من حيث وجودها من عدمه. الآن ولأول مرة سوف نقيّد الحقل F ـ بصورة عامة سيكون هو حقل الأعداد المركبة ولكن في بعض الأحيان نقصره على حقل الأعداد الحقيقية ـ وسوف نستعمل بكثرة خواص الأعداد الحقيقية والمركبة. *في كل ما سيأتي في هذا البند سيرمز F لحقل الأعداد المركبة، إلا إذا ذُكِرَ خلاف ذلك.*

وسـوف نستخدم بصورة دائمة جميع المفاهيم والنتائج المذكورة في بند (٤-٤) المتعلقة بفضاءات الضرب الداخلي. إننا ننصح القارىء بمراجعة تلك المادة وفهمها فهمًا تامًّا قبل المضي في القراءة.

نود أن نذكر ملاحظة أخرى عن الأعداد المركبة: استطعنا حتى الآن أن نتجنب استعمال نتائج لم نبرهنها في هذا الكتاب. ولكننا الآن مجبرون أن نحيد عن هذه الطريقة فنستعين بحقيقة أساسية عن الأعداد المركبة. تسمى عادة **«المبرهنة الأساسية في الجبر»**

(fundamental theorem of algebra) دون أن نبرهنهـــا. إن استعـــال هذه النتيجـة الأسـاسية كحقيقة دون برهان أمر لا يبعث على السرور. لسوء الحظ إنها ضرورية لدراسة ما سيأتي ولكن برهانها سيخرج بنا عن المسار العام في دراستنا الحالية. إننا نأمل أن يكون غالبية القرّاء قد رأوا برهانها في مقرر نظرية المتغير المركب.

حقيقة (١)

جميع جذور كثيرة الحدود التي معاملاتها أعداد مركبة تقع في حقل الأعداد المركبة.

بصـورة مكافئة يمكن كتابة حقيقة (١) على الصيغة: إن كثيرات الحدود غير الثـابتة وغير المختزلة على حقل الأعداد المركبة هي فقط كثيرات الحدود التي درجتها تساوي 1.

حقيقة (٢)

كثـيرات الحدود غير الثابتة وغير المختزلة على حقل الأعداد الحقيقية هي التي درجتها تساوي 1 أو التي درجتها تساوي 2.

إن صيغة إيجاد جذور المعادلة التربيعية تمكننا أن نبرهن بسهولة تكافؤ حقيقة (١) وحقيقة (٢).

إن ما تقتضيه حقيقة (١) بالنسبة لنا، *أنه لأي تحويل خطي ندرسه هنا ستكون جذوره المميزة في حقل الأعداد المركبة.*

فيما سيأتي، V سبر مز لفضاء ضرب داخلي منتهي البعد على F حقل الأعداد المركبة. سنكتب حاصل الضرب الداخلي لعنصرين v و w في V على الهيئة (v,w) كما فعلنا سابقا.

تمهيدية (٦-١٠-١)

إذا كان T في $A(V)$ بحيث $(vT,v)=0$ لكل v في V فإن $T=0$.

البرهان

لما كان $(vT,v)=0$ لكل v في V فإن $((u+w)T,u+w)=0$. بفك هذا المقدار واستعمال حقيقة أن

$$(uT,u)=(wT,w)=0$$

نحصل على:

$$(uT,w)+(wT,u)=0 \qquad (١)$$

لجميع u و w في V.

لما كانت المعادلة (١) صحيحة لعنصر اختياري w في V فإنها تبقى صحيحة إذا أبدلناه بالعنصر iw حيث $i^2=-1$.

ولكن

$$(uT,iw)=-i(uT,w)$$

بينما

$$((iw)T,u)=i(wT,w)$$

بتعويض هذه المقادير في (١) وحذف i نحصل على:

$$-(uT,w)+(wT,u)=0 \qquad (٢)$$

بجمع (١) و(٢) نحصل على

$$(wT,u)=0 \qquad \text{لكل } u \text{ و } w \text{ في } V.$$

وعلى وجه الخصوص يكون

$$(wT,wT)=0$$

باستخدام خواص فضاء الضرب الداخلي يقودنا هذا إلى أن يكون $wT=0$ لكل w في V ، وعليه يكون $T=0$. (**ملاحظة**: إذا كان V فضاء ضرب داخلي على حقل الأعداد الحقيقية فقد تكون التمهيدية خاطئة. **فعلى سبيل المثال** دع

$$V=\{(\alpha,\beta) \mid \alpha,\beta \text{ أعداد حقيقية}\}$$

حيث الضرب الداخلي هو الضرب النقطي المعتاد. ودع T ترمز للتحويل الخطي الذي

يرسل (α,β) إلى $(-\beta,\alpha)$. يمكن التأكد بسهولة أن $(vT,v)=0$ لكل v في V بالرغم من أن $(T\neq0$.

تعريف

يُدعى التحويل الخطي T في $A(V)$ واحديًا (unitary) إذا كان $(uT,vT)=(u,v)$ لكل u و v في V.

إن التحويل الواحدي هو تحويل يحفظ كل بنية V من جمع وضرب بالقياسيات بالاضافة *إلى ضربه الداخلي*. لاحظ أن التحويل الواحدي يحفظ الطول لأن

$$\|v\|=\sqrt{(v,v)}=\sqrt{(vT,vT)}=\|vT\|$$

هل العكس صحيح؟ إن التمهيدية التالية تجيب على هذا السؤال.

تمهيدية (٦-١٠-٢)

إذا كان $(vT,vT)=(v,v)$ لكل v في V فإن T تحويل واحدي.

البرهان

إن البرهان مشابه لبرهان تمهيدية (٦-١٠-١). ليكن u و v في V ومن الفرض يكون

$$((u+v)T,(u+v)T)=(u+v,u+v)$$

بفك هذا المقدار وتبسيطه نحصل على:

$$(uT,vT)+(vT,uT)=(u,v)+(v,u) \quad (١)$$

لكل u و v في V. في معادلة (١) ضع iv بدلا من v وأجر الحسابات اللازمة لتحصل على

$$-(uT,vT)+(vT,uT)=-(u,v)+(v,u) \quad (٢)$$

بجمع (١) و(٢) نحصل على $(uT,vT)=(u,v)$ لكل u و v في V، ويكون T تحويل واحدي.

الآن نضيف خاصة كون تحويل خطي واحديًا بدلالة تأثيره على أساس لـ V.

مبرهنة (٦-١٠-١)

يكون التحويل الخطي T على V واحديًا إذا وفقط إذا كان يأخذ أساسًا متعامدًا معايرًا لـ V إلى أساس متعامد معاير لـ V.

البرهان

لنفرض أن $\{v_1,\ldots,v_n\}$ أساس متعامد معاير لـ V ، لذا $(v_i,v_j)=0$ لكل $i\neq j$ بينما $(v_i,v_i)=1$. نود أن نثبت أنه إذا كان T تحويلاً واحديًا فإن $\{v_1T,\ldots,v_nT\}$ أساس متعامد معاير لـ V. ولكن $(v_iT,v_jT)=(v_i,v_j)=0$ لكل $i\neq j$ و $(v_iT,v_iT)=(v_i,v_i)=1$. لذا يكون $\{v_1T,\ldots,v_nT\}$ حقا أساسًا متعامدًا معايرًا لـ V.

من ناحية أخرى إذا كان T في $A(V)$ بحيث أن كلا من $\{v_1,\ldots,v_n\}$ و $\{v_1T,\ldots,v_nT\}$ أساس متعامد معاير لـ V فإنه لكل u و w في V يكون

$$u=\sum_{i=1}^{n}\alpha_i v_i \ \text{،}\ w=\sum_{i=1}^{n}\beta_i v_i$$

وباستعمال خاصة التعامد المعاير للمتجهات v_i نحصل على

$$(u,w)=\sum_{i=1}^{n}\alpha_i\bar{\beta}_i$$

ولكن

$$wT=\sum_{i=1}^{n}\beta_i v_i T \ \text{،}\ uT=\sum_{i=1}^{n}\alpha_i v_i T$$

واستنادًا لخاصة التعامد المعاير للمتجهات v_iT نحصل على

$$(uT,wT)=\sum_{i=1}^{n}\alpha_i\bar{\beta}_i=(u,w)$$

مما يبرهن على أن T تحويل واحدي.

إن مبرهنة (٦-١٠-١) تنص على أن التغيير من أساس متعامد معاير إلى آخر يتم بواسطة تحويل خطي واحدي.

تمهيدية (٦-١٠-٣)

إذا كان T في $A(V)$ فإنه لأي v في V يوجد عنصر w في V يعتمد على v و T بحيث $(uT,v)=(u,w)$ لكل u في V. إن العنصر w وحيد لكل اختيار لـ v و T.

البرهان

من أجل برهان التمهيدية، يكفي أن تجد عنصرا w في V يحقق استنتاج التمهيدية بالنسبة لأساس ما لـ V. ليكن $\{u_i,\ldots,u_n\}$ أساسًا متعامدًا معايرًا لـ V ونعرف

$$w=\sum_{i=1}^{n}\overline{(u_iT,v)}u_i$$

إن حسابًا بسيطًا يبين أن $(u_i,w)=(u_iT,v)$ مما يجعل w العنصر المطلوب. من أجل إثبات أن w وحيد نفرض أن

$$(uT,v)=(u,w_1)=(u,w_2)$$

فنستنتج أن

$$(u,w_1-w_2)=0$$

لكل u في V. وعندما نجعل $u=w_1-w_2$ نحصل على $w_1=w_2$.

إن تمهيدية (٦-١٠-٣) تمكننا من إعطاء التعريف التالي.

تعريف

*إذا كان T في $A(V)$ فإن **القرين الهرميتي** (Hermitian adjoint) لـ T ونرمز له بـ T^* يعرف بـ*

$$(uT,v)=(u,vT^*) \text{ لكل } u \text{ و } v \text{ في } V$$

لكل v في V حصلنا أعلاه على تعبير صريح لـ vT^* (على شكل w) ويمكننا استعمال ذلك التعبير لبرهان خصائص عديدة ومرغوبة لـ T^*، لكننا نفضل أن نفعل ذلك بصورة لا تعتمد على أساس V.

تمهيدية (٦-١٠-٤)

إذا كان T في $A(V)$ فإن T^* في $A(V)$ وبالإضافة إلى ذلك

١ - $(T^*)^*=T$

٢ - $(S+T)^*=S^*+T^*$

٣ - $(\lambda S)^*=\bar{\lambda}S^*$

٤ - $(ST)^*=T^*S^*$

لكل S ، T في $A(V)$ وكل λ في F.

البرهان

يجب أن نبرهن أولاً على أن T^* تحويل خطي على V. إذا كان u ، v و w في V فإن

$$(u,(\lambda v+w)T^*)=(uT,v+w)=(uT,v)+(uT,w)=(u,vT^*)+(u,wT^*)=(u,vT^*+wT^*)$$

وينتج عن ذلك أن

$$(v+w)T^*=vT^*+wT^*$$

وبصورة مشابهة، لكل λ في F

$$(u,(\lambda v)T^*)=(uT,\lambda v)=\bar{\lambda}(uT,v)=\bar{\lambda}(u,vT^*)=(u,\lambda(vT^*))$$

وعليه يكون $(\lambda v)T^*=\lambda(vT^*)$. لذا نكون قد برهنا على أن T^* تحويل خطي على V.

من أجل إثبات أن $(T^*)^*=T$ لاحظ أن

$$(u,v(T^*)^*)=(uT^*,v)=\overline{(v,uT^*)}=\overline{(vT,u)}=(u,vT)$$

لكل u و v في V وعليه $v(T^*)^*=vT$ والذي يقتضي أن يكون $(T^*)^*=T$. نترك برهان أن $(S+T)^*=S^*+T^*$ وأن $(\lambda T)^*=\bar{\lambda}T^*$ كتمرين للقارىء. أخيرا

$$(u,v(ST)^*)=(uST,v)=(uS,vT^*)=(u,vT^*S^*)$$

لكل u و v في V. وهذا يجعل $v(ST)^*=vT^*S^*$ لكل v في V وينتج عنه أن $(ST)^*=T^*S^*$.

كنتيجة للتمهيدية نجد أن القرين الهرميتي يعرِّف قرينًا على $A(V)$ في المفهوم المذكور في بند (٦-٨).

إن القرين الهرميتي يتيح لنا وصفًا آخر للتحويلات الواحدية بدلالة العلاقة بين T و *T.

تمهيدية (٦-١٠-٥)

يكون T في A(V) واحديًّا إذا وفقط إذا كان TT=1*

البرهان

إذا كان T واحديًّا فلكل u و v في V.

$$(u,vTT^*)=(uT,vT)=(u,v)$$

مما يجعل TT*=1. ومن جهة أخرى إذا كان TT*=1 فإن

$$(u,v)=(u,vTT^*)=(uT,vT)$$

والذي يقتضي أن T واحدي.

لاحظ أن التحويل الواحدي غير شاذ وأن معكوسه هو قرينه الهرميتي. لاحظ أيضًا أنه إذا كان TT*=1 فيجب أن يكون T*T=1. سوف نقدم أدناه معيارًا واضحًا بدلالة المصفوفات لكون تحويل خطي واحديًّا.

مبرهنة (٦-١٠-٢)

*إذا كان $\{v_1,\ldots,v_n\}$ أساسًا متعامدًا معايرًا لـ V وكانت (α_{ij}) مصفوفة T في A(V) بالنسبة لهذا الأساس فإن مصفوفة *T بالنسبة لهذا الأساس هي (β_{ij}) حيث $\beta_{ij}=\overline{\alpha_{ji}}$.*

البرهان

لما كانت مصفوفتا T و *T ، بالنسبة لهذا الأساس، هما (α_{ij}) و (β_{ij}) على الترتيب فإن

$$v_iT^*=\sum_{i=1}^{n}\beta_{ij}v_j \quad \text{و} \quad v_iT=\sum_{i=1}^{n}\alpha_{ij}v_j$$

الآن

$$\beta_{ij}=(v_iT^*,v_j)=(v_i,v_jT)=(v_i,\sum_{k=1}^{n}\alpha_{jk}v_k)=\bar{\alpha}_{ji}$$

وذلك استنادًا لخاصة التعامد المعاير لـ $\{v_1,\ldots,v_n\}$.

إن هذه المبرهنة شيّقة جدًّا وذلك في ضوء ما عملناه سابقًا في بند (٦ـ٨) ذلك لأن القرين الهرميتي المعرف على فضاء الضرب الداخلي V مكتوب بدلالة المصفوفات بالنسبة لأساس متعامد معاير في V ، هو ليس إلا القرين الهرميتي للمصفوفات المعرف في ذلك البند.

باستخدام المصفوفات بالنسبة إلى أساس متعامد معاير فإننا ندعي أن T في A(V) واحدي إذا وفقط إذا حققت عناصر مصفوفة T ولتكن (α_{ij}) ما يلي:

$$\sum_{i=1}^{n}\alpha_{ij}\,\bar{\alpha}_{ik}=0 \qquad \text{حيث } j\neq k$$

و

$$\sum_{i=1}^{n}|\alpha_{ij}|^2=1$$

بدلالة الضرب النقطي على فضاء المتجهات المركب فإن الشرطين أعلاه ينصان على أن صفوف مصفوفة T تكون مجموعة متعامدة معايرة من متجهات في $F^{(n)}$ نسبة إلى هذا الضرب النقطي.

تعريف

يسمى T في A(V) ***قرينًا ذاتيًّا*** *(self-adjoint)* ***أو هرميتيًّا*** *(Hermitian) إذا كان $T^*=T$. وإذا كان $T^*=-T$ فندعوه حينئذ هرميتيًّا تخالفيًّا.* إذا كان S في A(V) فإن

$$S=\frac{S+S^*}{2}+i\left(\frac{S-S^*}{2i}\right)$$

وحيث إن $(S+S^*)/2$ و $(S-S^*)/2i$ هرميتيان فإن $S=A+iB$ حيث إن كلا من A و B هرميتي.

في بنـد (٦ـ٨) وبـاستخدام حسابات المصفوفات برهنا على أن أي جذر مميز لمصفوفة هرميتية في الأعداد المركبة هو عدد حقيقي. على ضوء حقيقة (١) يمكن إعادة صياغة ذلك ليصبح : *جميع الجذور المميزة لمصفوفة هرميتية هي أعداد حقيقية*. الآن نعيد برهان ذلك من وجهة نظر فضاءات الضرب الداخلي.

مبرهنة (٦ـ١٠ـ٣)

إذا كان T في $A(V)$ هرمتيًّا فإن جميع جذوره المميزة أعداد حقيقية.

البرهان

ليكن λ جذرًا مميزًا لـ T، عندئذ يوجد $v\neq 0$ في V بحيث $vT=\lambda v$. الآن نحسب

$$\lambda(v,v)=(\lambda v,v)=(vT,v)=(v,vT^*)=(v,vT)$$
$$=(v,\lambda v)=\bar{\lambda}(v,v)$$

ولكن $(v,v)\neq 0$ مما يجعل $\lambda=\bar{\lambda}$ أي λ عدد حقيقي.

إننـا نرغب في أن نصف صيغًا قانونية للتحويلات الخطية الواحدية والهرميتية وحتى التحويلات الأكثر عمومية التي ستكون أبسط من صيغة جوردان. إن هذا هو الغرض من التمهيديات القليلة القادمة التي على الرغم من كونها مشوّقة بحد ذاتها إلا أنها غالبا ما تكون ذات طبيعة حسابية تخدم غرضًا معينًا.

تمهيدية (٦ـ١٠ـ٦)

إذا كان S في $A(V)$ وكان $vSS^*=0$ فإن $vS=0$.

البرهان

لنعتبر (vSS^*,v). لما كان $vSS^*=0$ عندئذ $0=(vSS^*,v)=(vS,v(S^*)^*)=(vS,vS)$ وذلك باستخدام تمهيدية (٦ـ١٠ـ٤) ونستنتج من ذلك أن $vS=0$ لأننا في فضاء ضرب داخلي.

نتيجة

إذا كان T هرميتيًا وكان $vT^k=0$ لـ $k\geqslant 0$ فإن $vT=0$.

البرهان

نثبت أولا أنه إذا كان $vT^{2m}=0$ فإن $vT=0$. فلو كان $S=T^{2m-1}$ فإن $S^*=S$ و $SS^*=T^{2m}$ وعليه $(vSS^*,v)=0$ يقتضي أن يكون $0=vS=vT^{2m-1}$. بالاستمرار نزولا، على هذا النحو نحصل على $vT=0$. إذا كان $vT^k=0$ فإن $vT^{2m}=0$ لـ $2^m>k$ وهذا يجعل $vT=0$.

الآن نقـدم نوعا من التحويلات الخطية يحوي كلًّا من التحويلات الواحدية والهرميتية والهرميتية المتخالفة كحالات خاصة.

تعريف

يُطلق على T في $A(V)$ تحويل خطي ناظمي ***(normal linear transformation)*** *إذا كان $TT^*=T^*T$.*

فيما سيأتي سنبرهن مبرهنات حول التحويلات الخطية الناظمية بدلاً من برهانها في حالة التحويلات الواحدية والهرميتية، ثم نشتق النتائج المرغوبة حول التحويلات الواحدية والهرميتية كحالتين خاصتين.

تمهيدية (٦-١٠-٧)

إذا كان N تحويلًا خطيًّا ناظميًّا وكان $vN=0$ لـ v في V فإن $vN^*=0$.

البرهان

لنعتبر (vN^*,vN^*). باستخدام التعريف ولكون $NN^*=N^*N$ نحصل على:

$$(vN^*,vN^*)=(vN^*N,v)=(vNN^*,v)$$

ولكن $vN=0$ مما يجعل $vNN^*=0$. وبذا نستنتج أن $(vN^*,vN^*)=0$ وبالتالي $vN^*=0$.

نتيجة (١)

إذا كان λ جذرًا مميزًا للتحويل الناظمي N وكان $vN=\lambda v$ فإن $vN^*=\bar{\lambda}v$.

البرهان

لما كان N ناظميا فإن $NN^*=N^*N$.

إذن

$$(N-\lambda)(N-\lambda)^*=(N-\lambda)(N^*-\bar{\lambda})=NN^*-\lambda N^*-\bar{\lambda}N+\lambda\bar{\lambda}=N^*N-\lambda N^*-\bar{\lambda}N+\lambda\bar{\lambda}$$
$$=(N^*-\bar{\lambda})(N-\lambda))=(N-\lambda)^*(N-\lambda)$$

وهذا يجعل $(N-\lambda)$ ناظميًّا. وحيث إن $v(N-\lambda)=0$ ولكون $(N-\lambda)$ ناظميًّا نستنتج أن $v(N-\lambda)^*=0$ باستخدام التمهيدية. وعليه يكون $vN^*=\bar{\lambda}v$.

إن النتيجة تنص على الحقيقة الشيّقة وهي إذا كان λ جذرًا مميزًا للتحويل الناظمي N فليس $\bar{\lambda}$ جذرًا مميزًا لـ N^* فحسب، ولكن أي متجه مميز لـ N يتبع الجذر المميز λ هو متجه مميز لـ N^* يتبع $\bar{\lambda}$ والعكس بالعكس.

نتيجة (٢)

إذا كان T واحديًا وكان λ جذرًا مميزًا لـ T فإن $|\lambda|=1$.

البرهان

لما كان T واحديًّا فإنه ناظمي. ليكن λ جذرًا مميزًا لـ T ولنفرض أن $vT=\lambda v$ حيث $v\neq 0$ في V. وفقًا لنتيجة (١) يكون $vT^*=\bar{\lambda}v$ لذا $v=vTT^*=\lambda vT^*=\lambda\bar{\lambda}v$ لأن $TT^*=1$. نستنتج أن $\lambda\bar{\lambda}=1$ وهذا يعني أن $|\lambda|=1$.

الآن نتوقف لنعرف وجهتنا. إن هدفنا القريب هو برهان أنه يمكن الحصول على صيغة قطرية لتحويل ناظمي بواسطة تحويل واحدي. إذا كانت $\lambda_1,\ldots,\lambda_k$ جذورا مميزة مختلفة لـ N فباستخدام مبرهنة (٦-٦-١) يمكننا تفريق V على النحو $V=V_1\oplus\ldots\oplus V_k$ حيث $v_i(N-\lambda_i)^{n_i}=0$ لكل v_i في V_i. في هذا الصدد سندرس شيئين: **أولهما** علاقة

المتجهات الموجودة في V_i مع المتجهات في V_j حيث $i\neq j$ ، **وثانيهما** طبيعة كل من الفضاءات V_i. عندما ننتهي من ذلك سنتمكن من جمع الحقائق لإثبات المبرهنة التي ننشدها.

تمهيدية (٦-١٠-٨)

إذا كان N ناظميًا وكان $vN^k=0$ فإن $vN=0$.

البرهان

ليكن $S=NN^*$ فيكون S هرميتيًا. وحيث إن N ناظمي يصبح

$vS^k=v(NN^*)^k=vN^k(N^*)^k=0$.

باستخدام نتيجة تمهيدية (٦-١٠-٦) نستنتج أن $vS=0$ ، أي أن $vNN^*=0$ وهذا يجعل $vN=0$ وفقا لتمهيدية (٦-١٠-٦).

نتيجة

إذا كان N ناظميًا و λ في F بحيث $v(N-\lambda)^k=0$ فإن $vN=\lambda v$.

البرهان

لكون N ناظميًا نستنتج أن $(N-\lambda)$ ناظمي وعليه فبتطبيق التمهيدية التي خلصنا من برهانها على $(N-\lambda)$ نحصل على النتيجة.

على ضوء ما ذكرناه قبل التمهيدية الأخيرة فإن هذه النتيجة تبين أن *كل متجه في V_i هو متجه مميز لـ N يتبع الجذر المميز λ_i*. بهذا نكون قد عيّنا طبيعة V_i ، أما الآن فإننا نمضي لدراسة العلاقة بين V_i و V_j حيث $i\neq j$.

تمهيدية (٦-١٠-٩)

إذا كان N تحويلا ناظميا وكان λ و μ جذرين مميزين مختلفين لـ N. وإذا كان v و w في V بحيث $vN=\lambda v$ و $wN=\mu w$ فإن $(v,w)=0$.

البرهان

نحسب (vN,w) بطريقتين مختلفتين. بما أن $vN=\lambda v$ فإن $(vN,w)=(hv,w)=h(v,w)$.
كذلك بما أن $wN=\mu w$ واستناداً إلى تمهيدية (٦-١٠-٧) نحصل على $wN^*=\bar{\mu}w$ وعليه فإن $(vN,w)=(v,wN^*)=(v,\bar{\mu}w)=\mu(v,w)$. بمقارنة نتيجتي الحساب نحصل على $\lambda(v,w)=\mu(v,w)$ ولكون $\lambda\neq\mu$ نخلص إلى أن $(v,w)=0$.

الآن نكون قد أنجزنا الخلفية اللازمة التي تمكننا من برهان المبرهنة الأساسية التالية.

مبرهنة (٦-١٠-٤)

إذا كان N تحويلاً خطيًّا ناظميًّا على V ، فإنه يوجد أساس متعامد معاير مكون من متجهات مميزة لـ N وفيها تكون مصفوفة N قطرية. وبعبارة مكافئة، إذا كانت N مصفوفة ناظمية فإنه توجد مصفوفة واحدية U بحيث تكون $UNU^{-1}(=UNU^*)$ مصفوفة قطرية.

البرهان

سنكمل تفاصيل البرهان الذي قدمنا له قبل إثبات تمهيدية (٦-١٠-٨).
ليكن N تحويلاً ناظميًّا و $\lambda_1,\ldots,\lambda_k$ الجذور المميزة المختلفة لـ N. استنادا لنتيجة مبرهنة (٦-٦-١) يمكننا تفريق V على الهيئة $V=V_1\oplus\ldots\oplus V_k$ حيث لكل v_i في V_i يكون $v_i(N-\lambda_i)^{n_1}=0$. باستخدام نتيجة تمهيدية (٦-١٠-٨) فإن V_i يحوي فقط على متجهات مميزة لـ N تابعة للجذر المميز λ_i. إن الضرب الداخلي في V ينتج عنه ضرب داخلي في V_i وباستعمال مبرهنة (٤-٤-٢) يمكننا إيجاد أساس متعامد معاير لـ V_i بالنسبة لهذا الضرب الداخلي.

وفقا لتمهيدية (٦-١٠-٩) فإن المتجهات الموجودة في V_i عمودية على المتجهات في V_j طالما أن $i\neq j$. لذا فبتجميع الأساسات المتعامدة المعايرة من كل V_i نحصل على

أساس متعامد معاير لـ V. إن هذا الأساس مكوّن من متجهات مميزة لـ N وعليه تكون مصفوفة N بالنسبة لهذا الأساس قطرية.

سوف لا نبرهن العبارة المكافئة والخاصة بالمصفوفات ونتركها كمسألة للقارىء ونكتفي بالإشارة إلى الحاجة إلى الحقيقتين التاليتين:

١ - إن تغيير الأساس من أساس متعامد معاير إلى آخر يتم عن طريق تحويل واحدي (مبرهنة ٦-١٠-١).

٢ - عند تغيير الأساس فإن مصفوفة التحويل الخطي تتحول إلى مصفوفة مرافقة عن طريق مصفوفة تغيير الأساس (مبرهنة ٦-٣-٢).

إن النتيجتين التاليتين هما حالتان خاصتان جدا من مبرهنة (٦-١٠-٤) ولكن لكون كل منهما مهمة بحد ذاتها فإننا ننص عليهما كنتيجتين لغرض التأكيد عليهما.

نتيجة (١)

إذا كان T تحويلًا واحديًا فإنه يوجد أساس متعامد معاير والذي فيه تكون مصفوفة T قطرية. بعبارة مكافئة، إذا كانت T مصفوفة واحدية فإنه توجد مصفوفة واحدية U بحيث تكون $UTU^{-1}(=UTU^{*})$ مصفوفة قطرية.

نتيجة (٢)

إذا كان T تحويلًا خطيًا هرميتيًا فإنه يوجد أساس متعامد معاير والذي فيه تكون مصفوفة T قطرية. وبعبارة مكافئة، إذا كانت T مصفوفة هرميتية فإنه توجد مصفوفة واحدية U بحيث تكون $UTU^{-1}(=UTU^{*})$ مصفوفة قطرية.

إن المبرهنة التي انتهينا من برهانها تعتبر نتيجة أساسية في التحويلات الناظمية لأنها تميز تلك التحويلات بأنها التحويلات التي يمكن تغييرها إلى الصيغة القطرية عن طريق تحويلات واحدية. كما أن المبرهنة تبين أن الفرق بين التحويلات الناظمية والهرميتية يكمن في طبيعة جذورها المميزة. ونوضح هذا في التمهيدية التالية.

تمهيدية (٦-١٠-١٠)

يكون التحويل الناظمي N:

١ ـ هرميتيًا إذا وفقط إذا كانت جذوره المميزة حقيقية.

٢ ـ واحديًا إذا وفقط إذا كانت القيمة المطلقة لكل جذوره المميزة تساوي 1.

البرهان

تستعمل المصفوفات في مناقشتنا. إذا كانت N هرميتية فإنها ناظمية وجميع جذورها المميزة حقيقية. إذا كانت N ناظمية وكانت جذورها المميزة حقيقية فإنه توجد مصفوفة واحدية U بحيث تكون

$$UNU^{-1}=UNU^{*}=D$$

حيث D مصفوفة قطرية فيها عناصر القطر أعداد حقيقية. لذا $D^*=D$. ولما كانت

$$D^*=(UNU^*)^*=UN^*U^*$$

فإن العلاقة $D^*=D$ تقتضي أن تكون $UN^*U^*=UNU^*$. وحيث إنه يوجد معكوس لـ U فإننا نحصل على أن $N^*=N$. لذا تكون N هرميتية.

نترك برهان الجزء الخاص بالتحويل الواحدي للقارىء.

إذا كان A أي تحويل خطي على V فإنه يمكن حساب $tr(AA^*)$ باستخدام مصفوفة A نسبة لأي أساس لـ V. لنختار أساسًا متعامدًا معايرًا لـ V. في هذا الأساس إذا كانت مصفوفة A هي (α_{ij}) فإن مصفوفة A^* هي (β_{ij}) حيث $\beta_{ij}=\bar{\alpha}_{ji}$. إن حسابا بسيطًا يبين لنا أن $tr(AA^*)=\Sigma_{i,j}|\alpha_{ij}|^2$ وهذا يساوي صفرا إذا وفقط إذا كان كل α_{ij} يساوي صفرا، أي إذا وفقط إذا كان $A=0$. وباختصار $tr(AA^*)=0$ إذا وفقط إذا كان $A=0$. إن هذا معيار مفيد لبيان كون تحويل خطي مساويًا للصفر. ويتضح هذا في التمهيدية التالية.

تمهيدية (٦-١٠-١١)

إذا كان N تحويلًا ناظميًا وكان $AN=NA$ فإن $AN^*=N^*A$.

البرهان

إننا نريد أن نبين أن $X=AN^*-N^*A$ يساوي صفرا. إن ما سنفعله هو برهان أن $trXX^*=0$ فنستنتج من ذلك أن $X=0$.

لما كان N يتبادل مع A ومع N^* فإنه يجب أن يتبادل مع AN^*-N^*A، لذا

$$XX^*=(AN^*-N^*A)(NA^*-A^*N)=(AN^*-N^*A)NA^*-(AN^*-N^*A)A^*N$$
$$=N((AN^*-N^*A)A^*)-((AN^*-N^*A)A^*)N$$

ونستنتج من ذلك أن $trXX^*=0$ لأن X هو على الصيغة $NB-BN$. لذا $X=0$ وبالتالي فإن $AN^*=N^*A$.

لقد بيّنا أن N^* يتبادل مع جميع التحويلات الخطية التي تتبادل مع N حيث N تحويل ناظمي. إن هذا كافٍ ليجعل N^* يساوي كثيرة حدود من N. بيد أنه يمكن برهان ذلك مباشرة كاستنتاج من مبرهنة (٦-١٠-٤) (انظر مسألة ١٤).

يكون التحويل الخطي T هرميتيًّا إذا وفقط إذا كان (vT,v) عددًا حقيقيًّا لكل v في V. (انظر مسألة ١٩). من التحويلات الهرميتية ذات الأهمية الخاصة تلك التي يكون فيها $(vT,v)\geqslant 0$ لكل v في V. ندعو تلك التحويلات بالتحويلات الخطية **غير السالبة** (nonnegative) ونرمز لها بالرمز $T\geqslant 0$. إذا كان $T\geqslant 0$ وكان $(vT,v)>0$ لـ $v\neq 0$ فعندئذ نقول عن T **انه موجب (أو موجب بالتحديد)** positive (positive definite) ونكتب ذلك على الصيغة $T>0$. إننا نرغب في التعرف على هذه التحويلات الخطية بواسطة جذورها المميزة.

تمهيدية (٦-١٠-١٢)

يكون التحويل الخطي الهرميتي غير سالب (موجبًا) إذا وفقط إذا كانت جميع جذوره المميزة غير سالبة (موجبة).

البرهان

لنفرض أن $T\geqslant 0$. إذا كان λ جذرا مميزا لـ T فإن $vT=\lambda v$ لمتجه $v\neq 0$. لذا

$$0\leqslant(vT,v)=(\lambda v,v)=\lambda(v,v)$$

وحيث إن $0<(v,v)$ نستنتج أن $\lambda\geqslant 0$.

ومن جهة أخرى إذا كان T هرميتيًا وكانت جميع جذوره المميزة غير سالبة فإنه بالإمكان إيجاد أساس متعامد معاير $\{v_1,\ldots,v_n\}$ يحوي على متجهات مميزة لـ T. لكل v_i يكون $v_iT=\lambda_iv_i$ حيث $\lambda_i\geqslant 0$. الآن لكل v في V، $v=\Sigma\alpha_iv_i$ وعليه

$$vT=\Sigma\alpha_iv_iT=\Sigma\lambda_i\alpha_iv_i$$

ولكن عندئذ يصبح

$$(vT,v)=(\Sigma\lambda_i\alpha_i\,v_i,\Sigma\alpha_1v_i)=\Sigma\lambda_i\alpha_i\bar{\alpha}_i$$

وذلك باستخدام خاصة التعامد المعاير للأساس $\{v_1,\ldots,v_n\}$. لما كانت $\lambda_i\geqslant 0$ و $\alpha_i\bar{\alpha}_1\geqslant 0$ فنحصل على $(vT,v)\geqslant 0$ أي $T\geqslant 0$.

نترك للقارىء كتمرين الجزء الخاص بالحالة الموجبة.

تمهيدية (٦-١٠-١٣)

يكون $T>o$ إذا وفقط إذا كان $T=AA^*$ حيث A تحويل خطي ما.

البرهان

أولاً نبيّن أن $AA^*\geqslant 0$. لكل v في V يكون $(vAA^*,v)=(vA,vA)\geqslant 0$ وعليه $AA^*\geqslant 0$.

ومن جهة أخرى، إذا كان $T\geqslant 0$ فبإمكاننا إيجاد مصفوفة واحدية U بحيث

$$UTU^*=\begin{pmatrix}\lambda_1 & & & & \\ & \lambda_2 & & & \\ & & \ddots & & \\ & & & & \\ & & & & \lambda_n\end{pmatrix}$$

حيث إن كل λ_i جذر مميّز لـ T وعليه فإن $\lambda_i \geq 0$ لكل i.

دع

$$S = \begin{pmatrix} \sqrt{\lambda_1} & & & & \\ & \sqrt{\lambda_2} & & & \\ & & \ddots & & \\ & & & & \sqrt{\lambda_n} \end{pmatrix}$$

لما كان $\lambda_i \geq 0$ لكل i فإن كلا من $\sqrt{\lambda_i}$ عدد حقيقي وبناء عليه تكون S هرميتية. إذن U*SU هرميتية. ولكن

$$(U^*SU)^2 = U^*S^2U = U^* \begin{pmatrix} \lambda_1 & & & & \\ & \lambda_2 & & & \\ & & \ddots & & \\ & & & & \lambda_n \end{pmatrix} U = T$$

بهذا نكون قد مثّلنا T على الصيغة *AA حيث A=U*SU.

لاحظ أننـا برهنّا على أكثر من نص التمهيدية. ونعني بذلك أنه عند إنشائنا لـ S أعـلاه لو اخـترنـا الجذر غير السالب $\sqrt{\lambda_i}$ لكل λ_i فحينئذ تكون S و U*SU غير سالبتين. لذا $T \geqslant 0$ هو مربع لتحويل خطي غير سالب، أي يوجد جذر تربيعي غير سالب لكل $T \geqslant 0$. يمكن البرهان على أن الجذر التربيعي غير السالب هذا وحيد (انظر مسألة ٢٤).

نختـم هذا البنـد بمنـاقشـة عن المصفـوفـات الواحدية والهرميتيـة على *حقل الأعداد الحقيقية*. في هذه الحالة تسمى المصفوفـات الواحديـة **مصفوفـات متعامـدة** (orthogonal matrices) وهي تحقق $QQ'=1$. أمـا المصفـوفات الهرميتية فهي في هذه الحالة المصفوفات المتناظرة.

إننا ندعي بأنه يمكن *تحويل أية مصفوفة حقيقية متناظرة إلى الصيغة القطرية بواسطة مصفوفة متعامدة*. لتكن A مصفوفة حقيقية متناظرة. يمكننا اعتبار A مصفوفة تعمل على فضاء الضرب الداخلي الحقيقي V. باعتبار A مصفوفة من أعداد مركبة فإنها هرميتية وعليه تكون جميع جذورها المميزة حقيقية. إذا كانت هذه الجذور هي $\lambda_1,\ldots,\lambda_k$ فيمكن تفريق V على الصيغة $V=V_1\oplus\ldots\oplus V_k$ بحيث $v_i(A-\lambda_i)^{n_i}=0$ لكل v_i في V_i. كما في برهان تمهيدية (٦-١٠-٨) نستنتج من هذا أن $v_iA=\lambda_iv_i$. باستخدام البرهان نفسه المستعمل في تمهيدية (٦-١٠-٩) نستطيع أن نبيّن أنه لـ v_i في V_i و v_j في V_j يكون $(v_i,v_j)=0$ حيث $i\neq j$. لذا يمكننا إيجاد أساس متعامد معاير لـ V يحوي على متجهات مميزة لـ A. إن تغيير الأساس من الأساس المتعامد المعاير$\{(1,0,\ldots,0),(0,1,\ldots,0)\ldots,(0,\ldots,0,1)\}$ إلى هذا الأساس الجديد يتم عن طريق مصفوفة واحدية حقيقية أي مصفوفة متعامدة. لذا يمكن تحويل A إلى الصيغة القطرية عن طريق مصفوفة متعامدة مما يثبت ادعاءنا أعلاه.

إن تعيين صيغة قانونية للمصفوفات المتعامدة الحقيقية على حقل الأعداد الحقيقية أمر فيه بعض التعقيد ليس في الصيغة نفسها بل في طريقة الحصول عليها أيضا. الآن نسير بهذا الاتجاه ولكننا أولاً نود تقديم ملاحظة عامة تتعلق بجميع التحويلات الواحدية.

إذا كان W فضاءً جزئيًا من V وكان W غير متغير تحت تأثير التحويل الواحدي T، فهل صحيح أن المتمم العمودي W' لـ W هو أيضا غير متغير تحت تأثير T ؟ دع w في W و x في W'، لذا $(wT,xT)=(w,x)=0$ ولما كان W غير متغير تحت T و T تحويل منتظم مما يجعل $WT=W$ وعليه xT عمودي على كل متجهات W لكل x في W'. إذن، $W'T\subset W'$ تذكر أن $V=W\oplus W'$.

لتكن Q مصفوفة متعامدة حقيقية. عندئذ، فإن

$$T=Q+Q^{-1}=Q+Q'$$

مصفوفة متناظرة وعليه تكون جذورها المميزة أعدادا حقيقية. إذا كانت تلك الجذور هي $\lambda_1,\ldots,\lambda_k$ فيمكن تفريق V إلى $V=V_1\oplus\ldots\oplus V_k$ حيث $v_iT=\lambda_iv_i$ لكل v_i في

V_i . إن الفضاءات الجزئية V_i متعامدة على بعضها . إننا ندّعي أن كلا من V_i غير متغير تحت تأثير Q (برهن على ذلك). لذا فلمناقشة عمل Q على V يكفينا أن نصف عملها على كل من V_i .

في V_i ، لما كان $\lambda_i v_i = v_i T = v_i(Q+Q^{-1})$ ، عند الضرب بـ Q نحصل على $v_i(Q^2-\lambda_i Q+1)=0$. هناك حالتان خاصتان لابد من الإشارة إليهما وهما عندما $\lambda_i=2$ و $\lambda_i=-2$ (وبالطبع ليس ضروريًا أن تحدث أي من تلكما الحالتين)، عندئذ $v_i(Q\pm1)^2=0$ وهذا يجعل $v(Q\pm1)=0$. في هذه الفضاءات تعمل Q كعمل 1 أو -1.

إذا كان $\lambda_i \neq 2,-2$ فعندئذ لا يوجد لـ Q متجهات مميزة في V_i وعليه يكون المتجهان v, vQ مستقلين خطيًا لكل $v\neq0$ في V_i. إن الفضاء الجزئي المولد منهما غير متغير تحت تأثير Q لأن $vQ^2=\lambda_i vQ-v$. الآن $V_i=W\oplus W'$ حيث W' غير متغير تحت تأثير Q. لذا يمكننا أن نحصل على V_i كحاصل جمع مباشر لفضاءين ثنائيي البعد متعامدين على بعضهما غير متغيرين تحت Q. كي نجد الصيغة القانونية لـ Q على V_i (وبالتالي V) بقي علينا أن ننجز حالة المصفوفات المتعامدة الحقيقية من نوع 2×2.

لتكن Q مصفوفة حقيقية متعامدة من نوع 2×2 تحقق $Q^2-\lambda Q+1=0$ ، لنفرض أن $Q=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$. إن تعامد Q يقتضي أن يكون

$$\alpha^2+\beta^2=1 \qquad (١)$$

$$\gamma^2+\delta^2=1 \qquad (٢)$$

$$\alpha\gamma+\beta\delta=0 \qquad (٣)$$

لما كان $Q^2-\lambda Q+1=0$ فإن محدّدة Q تساوي 1 ، وعليه

$$\alpha\delta-\beta\gamma=1 \qquad (٤)$$

إننا ندعي أن المعادلات من (١) إلى (٤) تقتضي أن يكون $\alpha=\delta$ و $\gamma=-\beta$. وحيث إن $\alpha^2+\beta^2=1$ مما يجعل $|\alpha|\leq1$ وعليه يمكننا كتابة $\alpha=\cos\theta$ لزاوية حقيقية ما θ ، وبهذه الدلالات يكون $\beta=\sin\theta$. إذن تصبح المصفوفة Q على الصيغة

$$\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$$

إن جميع الفضاءات التي استُخدمت في جميع عمليات التفريق كانت متعامدة على بعضها . لذا فباختبار الأساسات متعامدة معايرة لكل من تلك الفضاءات نحصل على أساس متعامد معاير لـ V. وفي هذا الأساس تكون مصفوفة Q على النحو الموضح في الشكل (٦-١-١)

$$\begin{pmatrix} \boxed{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}} & & & & \\ & \boxed{\begin{matrix} -1 & & \\ & \ddots & \\ & & -1 \end{matrix}} & & & \\ & & \boxed{\begin{matrix} \cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & \cos\theta_1 \end{matrix}} & & \\ & & & \ddots & \\ & & & & \boxed{\begin{matrix} \cos\theta_r & \sin\theta_r \\ -\sin\theta_r & \cos\theta_r \end{matrix}} \end{pmatrix}$$

شكل (٦-١٠-١)

وحيث أننا تحولنا من أساس متعامد معاير إلى آخر وأن هذا يتم بواسطة مصفوفة متعامدة . **لذلك نستنتج أنه** : إذا كانت Q مصفوفة حقيقية متعامدة فبإمكاننا إيجاد مصفوفة متعامدة T بحيث تكون $TQT^{-1}(=TQT^*)$ مصفوفة على الصيغة الموصوفة أعلاه .

مســائــل

١ - عين أيا من المصفوفات التالية : واحدية ، هرميتية ، ناظمية

(أ) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ ، (ب) $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ ، (جـ) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(د) $\begin{pmatrix} 1 & 2-i \\ 2-i & i \end{pmatrix}$ ، (هـ) $\begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$

٢ ـ أوجد الجذور المميزة للمصفوفات الناظمية من بين المصفوفات المذكورة في مسألة (١)، ثم حول تلك المصفوفات إلى الصيغة القطرية بواسطة مصفوفات واحدية.

٣ ـ إذا كان T تحويلاً واحديًا فأثبت باستخدام التعريف $(vT, uT)=(v,u)$ أن T غير شاذ.

٤ ـ إذا كانت Q مصفوفة حقيقية متعامدة. فبرهن على أن $\det Q=\pm 1$.

٥ ـ إذا كانت Q مصفوفة حقيقية متناظرة تحقق $Q^k=1$ لـ $k\geqslant 1$. فبرهن على أن $Q^2=1$.

٦ ـ أكمل برهان تمهيدية (٦ـ١٠ـ٤) بإثبات أن:

$$(S+T)^*=S^*+T^* \text{ و } (\lambda T)^*=\bar{\lambda}T^*$$

٧ ـ أثبت خواص * المذكورة في تمهيدية (٦ـ١٠ـ٤) باستعمال الصيغة الصريحة لـ $w=vT^*$ الواردة في برهان تمهيدية (٦ـ١٠ـ٣).

٨ ـ إذا كان T تحويلاً هرميتيًا تخالفيًا. برهن على أن جميع جذوره المميزة هي أعداد تخيلية.

٩ ـ إذا كانت T مصفوفة حقيقية متناظرة تخالفيًا من نوع $n\times n$. فبرهن على أنه إذا كان n عددًا فرديًا فإن $\det T=0$.

١٠ ـ باستخدام طرق حساب المصفوفات المباشرة. أثبت أن كل مصفوفة حقيقية متناظرة من نوع 2×2 يمكن أن تحوَّل إلى الصيغة القطرية بواسطة مصفوفة متعامدة.

١١ ـ أثبت برهان الجزء الخاص بالمصفوفات من مبرهنة (٦ـ١٠ـ٤) والذي سبق أن ذكرنا خطوطه العريضة.

١٢ ـ أثبت أن التحويل الناظمي يكون واحديًا إذا وفقط إذا كانت القيم المطلقة لجميع جذوره المميزة تساوي 1.

١٣ - إذا كان $N_1,...,N_k$ عددًا منتهيًا من التحـويلات الناظمية القابلة للإبدال فيما بينها . فبرهن على أنه يوجد تحويل واحدي T بحيث تكون TN_iT^{-1} كلها قطرية .

١٤ - إذا كان N تحويلاً ناظميًا. فبرهن على أن $N^*=p(N)$ لكثيرة حدود ما $p(x)$.

١٥ - إذا كان N تحويلاً ناظميًا وكان $AN=0$. فبرهن على أن $AN^*=0$.

١٦ - أثبت أن A تحويل ناظمي إذا وفقط إذا كان A يتبادل مع AA^*.

١٧ - إذا كان N ناظميًا. فبرهن على أن $N=\Sigma\lambda_iE_i$ حيث $E_i^2=E_i$ ، $E_i^*=E_i$ و λ_i هي الجذور المميزة لـ N. (يسمى هذا **بالتفريق الطيفي** لـ spectral resolution of N)

١٨ - إذا كان N تحويلاً ناظميًا على V وكانت $f(x)$ و $g(x)$ كثيرتى حدود أوليتين نسبيًا معاملاتها أعداد حقيقية .فبرهن على أنه إذا كان $vf(N)=0$ و $wg(N)=0$ حيث v و w في V فإن $(v,w)=0$.

١٩ - برهن على أن التحويل الخطي T على V هرميتي إذا وفقط إذا كان (vT,v) عددًا حقيقيًا لكل v في V.

٢٠ - برهن على أن $T>0$ إذا وفقط إذا كان T هرميتيًا وكانت جميع جذوره المميزة أعدادًا حقيقية موجبة .

٢١ - إذا كان $A\geqslant 0$ و $(vA,v)=0$. فبرهن على أن $vA=0$.

٢٢ - (ا) إذا كان $A\geqslant 0$ وكان A^2 يتبادل مع التحويل الهرميتي B فإن A يتبادل مع B.
(ب) أثبت الجزء (ا) حتى لو لم يكن B هرميتيًا.

٢٣ - إذا كان $A\geqslant 0$ و $B\geqslant 0$ و $AB=BA$. فبرهن على أن $AB\geqslant 0$.

٢٤ - إذا كان $A\geqslant 0$ فأثبت أنه يوجد لـ A جذر تربيعي وحيد غير سالب .

٢٥ - لتكن $A=(\alpha_{ij})$ مصفوفة حقيقية متناظرة من نوع $n\times n$. دع

$$A_s=\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1s} \\ \vdots & & \vdots \\ \alpha_{s1} & \cdots & a_{ss} \end{pmatrix}$$

(ا) إذا كانت $A>0$. فبرهن على أن $A_s>0$ لـ $s=1,2,...,n$.

(ب) إذا كانت $A>0$. فبرهن على أن $\det A_s>0$ لـ $s=1,2,...,n$.

(جـ) إذا كانت $\det A_s>0$ لكل $s=1,2,\ldots,n$. فأثبت أن $A>0$.

(د) إذا كانت $A\geqslant 0$. فبرهن على أن $A_s \geq 0$ لكل $s=1,2,\ldots,n$.

(هـ) إذا كانت $A \geq 0$ فبرهن على أن $\det A_s\geqslant 0$ لكل $s=1,2,\ldots,n$.

(و) أعط مثالا لمصفوفة حقيقية متناظرة A بحيث $\det A_s\geqslant 0$ لكل $s=1,2,\ldots,n$ ولكن A ليست غير سالبة .

٢٦ ـ أثبت أن أية مصفوفة عناصرها أعداد مركبة يمكن تحويلها إلى صيغة مثلثة بواسطة مصفوفة واحدية .

(٦ ـ ١١) الصيغ التربيعية الحقيقية

لننهي هذا الفصل بدراسة مختصرة للصيغ التربيعية على حقل الأعداد الحقيقية . ليكن V فضاء ضرب داخلي حقيقي و A تحويلاً خطيًا (حقيقيا) متناظرًا على V. يُطلق على الدالة الحقيقية القيم $Q(V)$ والمعرفة على V بواسطة $Q(v)=(vA,v)$ **الصيغة التربيعية** (quadratic form) المصاحبة لـ A.

إذا اعتبرنا ، وبدون مساس للعمومية ، أن المصفوفة $A=(\alpha_{ij})$ هي مصفوفة حقيقية متناظرة تؤثر على $F^{(n)}$ ، وكذلك إذا عرفنا الضرب الداخلي على $F^{(n)}$ للمتجهين $(\delta_1 , \ldots, \delta_n)$ و $(\gamma_1 , \ldots, \gamma_n)$ بأنه العدد الحقيقي $\delta_1\gamma_1+\delta_2\gamma_2+\ldots+\delta_n\gamma_n$ وإذا كان $v=(x_1,\ldots,x_n)$ متجه في $F^{(n)}$ فإنه يمكن أن نبين من خلال حسابات سهلة أن

$$Q(v)=(vA,v)=\alpha_{11}x_1^2+\ldots+\alpha_{nn}x_n^2+2\sum_{i<j}\alpha_{ij}x_ix_j$$

من ناحية أخرى إذا كانت لدينا أية دالة تربيعية في n من المتغيرات

$$\gamma_{11}x_1^2+\ldots+\gamma_{nn}x_n^2+2\sum_{i<j}\gamma_{ij}x_ix_j$$

معاملاتها γ_{ij} أعداد حقيقية فمن الواضح أنه يمكننا النظر إلى هذه الدالة على أنها الصيغة التربيعية المصاحبة للمصفوفة الحقيقية المتناظرة $C=(\gamma_{ij})$.

في الفضاء الإقليدي الحقيقي ذي البعد n تستخدم الدوال التربيعية المذكورة أعلاه لتعريف السطوح التربيعية . على سبيل المثال، في المستوى الحقيقي تُعطى

الصيغـة $[\alpha x^2 + \beta xy + \gamma y^2]$ قِطعـا مخروطيًّا (قـد يكون محوره الكبير مائلا). إنه ليس مستغربا أن نتوقع وجود علاقة وثيقة بين الخواص الهندسية لهذا القطع المخروطي وبين المصفوفة المتناظرة

$$\begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix}$$

التي تصحبها الصيغة التربيعية.

لنتذكر أنه في الهندسة التحليلية المبتدئة استخدمنا عملية تدوير المحاور لتحويل $\alpha x^2+\beta xy+\gamma y^2$ لتصبح في نظام المحاور الجديدة على الهيئة $\alpha_1(x')^2+\gamma_1(y')^2$. تذكر أن $\alpha_1+\gamma_1=\alpha+\gamma$ وأن $\alpha\gamma-\beta^2/4=\alpha_1\gamma_1$. وهكذا فإن α_1 و γ_1 هما الجذران المميزان للمصفوفة

$$\begin{pmatrix} \alpha & \beta/2 \\ \beta/2 & \gamma \end{pmatrix}$$

إن تدوير المحـاور هو مجرد تغيير للأسـاس بواسطة تحويل متعامد وأن ما عملناه في الهنـدسـة هو مجرد تحويل المصفـوفـة المتنـاظرة إلى صيغتها القطرية بواسطة مصفوفة متعامدة. إن طبيعة الصيغة $\alpha x^2+\beta xy+\gamma y^2$ كقطع مخروطي تتعين أساسًا بواسطة مقدار وإشارة جذريها المميزين γ_1 و α_1.

إن دراسة مشابهة يمكن إجراؤها لتصنيف السطوح التربيعية في الفضاء الثلاثي وبـالأحـرى السطوح التربيعية في الفضاء ذي البعد n. إن ما تعنيه الطبيعة الهندسية للسطح التربيعي المصاحب لـ

$$\alpha_{11}x_1^2+\ldots+\alpha_{nn}x_n^2+2\sum_{i<j}\alpha_{ij}x_ix_j$$

هو مقدار وإشارة الجذور المميزة للمصفوفة (α_{ij}). إذا أهملنا الانبساط النسبي للسطوح التربيعية (كمثال: إذا اعتبرنا القطع الناقص دائرة منبسطة) فإننا سنهمل قيمة الجذور المميزة غير المساوية للصفر ويبقى عامل تعيين شكل السطح التربيعي هو عدد الجذور المميزة المساوية للصفر وعدد الجذور التي تكون موجبة (أو سالبة).

إن هذه الأمور تبعث على دراسة ما يسمى **بقانون سيلفستر** (Sylvester) للقصور الذاتي كما أننا سنوضحها فيما سيأتي من شرح.

لتكن A مصفوفة حقيقية متناظرة و $Q(v)=(vA,v)$ الصيغة التربيعية المصاحبة لـ A. إذا كان T أي تحويل خطي حقيقي غير شاذ فإنه لأي v في $F^{(n)}$ يوجد w في $F^{(n)}$ بحيث أن $v=wT$. وعليه

$$(vA,v)=(wTA,wT)=(wTAT',w)$$

لذا فإن A و TAT' يعرفان أساسًا الصيغة التربيعية نفسها. إن هذا يدفعنا إلى التعريف التالي.

تعريف

يقال عن المصفوفتين الحقيقيتين المتناظرتين A و B إنهما ***متطابقتان (congruent)*** *إذا وُجدت مصفوفة حقيقية غير شاذة T بحيث $B=TAT'$*

تمهيدية (٦-١١-١)

علاقة التطابق هي علاقة تكافؤ.

البرهان

لنرمز للعلاقة A تطابق B بالرمز $A\cong B$

١ - $A\cong A$ لأن $A=1A1'$

٢ - إذا كانت $A\cong B$ فإن $B=TAT'$ حيث T غير شاذة وعليه $A=SBS'$ حيث $S=T^{-1}$. إذن $B\cong A$.

٣ - إذا كان $A\cong B$ و $B\cong C$ فإن $B=TAT'$ و $C=RBR'$ وعليه $C=RTAT'R'=(RT)A(RT)'$ مما يجعل $A\cong V$.

ولما كانت العلاقة تحقق خواص علاقة التكافؤ فإننا نكون بهذا قد برهنا التمهيدية.

إن المبرهنة الأساسية المتعلقة بالتطابق هي التي تهتم بعملية التعرف عليه وهذه محتواة في **قانون العطالة لسلفستر** (Sylvester's law of inertia)

مبرهنة (٦-١١-١)

إذا كانت A مصفوفة حقيقية متناظرة فإنه توجد مصفوفة غير شاذة T بحيث

$$TAT'=\begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$$

حيث I_r و I_s هما على الترتيب مصفوفة الوحدة من نوع $r\times r$ ونوع $s\times s$ وحيث 0_t هي المصفوفة الصفرية من نوع $t\times t$. إن فصل التطابق لـ A يتعين بالعددين الصحيحين $r+s$ وهو مرتبة (A(rank و $r-s$ ويسمى ***توقيع*** *(A(signature. أي تكون المصفوفتان الحقيقيتان المتناظرتان متطابقتين إذا وفقط إذا كان لهما المرتبة والتوقيع نفسهما .*

البرهان

لما كانت A متناظرة فإن جميع جذورها المميزة حقيقية . لتكن $\lambda_1,\ldots,\lambda_r$ جذورها المميزة الموجبة و $-\lambda_{r+1},\ldots,-\lambda_{r+s}$ جذورها السالبة . استنادًا إلى المناقشة الواردة في نهاية بند (٦-١٠) توجد مصفوفة حقيقية متعامدة C بحيث

$$CAC^{-1}=CAC'=\begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_r & & & & \\ & & & -\lambda_{r+1} & & & \\ & & & & \ddots & & \\ & & & & & -\lambda_{r+s} & \\ & & & & & & O_t \end{pmatrix}$$

حيث $t=n-r-s$. لتكن D المصفوفة الحقيقية القطرية الموضحة في شكل (٦-١١-١) .

$$D=\begin{pmatrix} \frac{1}{\sqrt{\lambda_1}} & & & & & \\ & \ddots & & & & \\ & & \frac{1}{\sqrt{\lambda_r}} & & & \\ & & & \frac{1}{\sqrt{\lambda_{r+1}}} & & \\ & & & & \ddots & \\ & & & & & \frac{1}{\sqrt{\lambda_{r+s}}} & \\ & & & & & & I_t \end{pmatrix}$$

شكل (٦-١١-١)

إن حسابا بسيطا يبين أن

$$DCAC'D' = \begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$$

لذا توجد مصفوفة على الشكل المطلوب في فصل تطابق A.

إن مهمتنا الآن هي بيان أن هذه المصفوفة هي المصفوفة الوحيدة التي هي على الصيغة نفسها في فصل تطابق A. وبصورة مكافئة أن :

$$M = \begin{pmatrix} I_{r'} & & \\ & -I_{s'} & \\ & & O_{t'} \end{pmatrix} \text{ و } L = \begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$$

متطابقتان فقط إذا كان $r=r'$ ، $s=s'$ و $t=t'$.

لنفرض أن $M=TLT'$ حيث T مصفوفة لها معكوس. إن مرتبة M تساوي مرتبة L وفقًا لتمهيدية (٦-١-٣). وحيث إن مرتبة M تساوي $n-t'$ ومرتبة L تساوي $n-t$ نستنتج أن $t=t'$.

لنفرض أن $r<r'$ ولما كان $n=r+s+t=r'+s'+t'$ وحيث إن $t=t'$ فيجب أن يكون $s>s'$.

ليكن U الفضاء الجزئي في $F^{(n)}$ الحاوي على جميع المتجهات على الصيغة

$$(\underbrace{0,\ldots,0}_{r},x_{r+1},\ldots,x_{r+s},\underbrace{0,\ldots,0}_{t})$$

إن بعد U يساوي s ولكل $u\neq 0$ في U يكون $(uL,u)<0$.

ليكن W الفضاء الجزئي في $F^{(n)}$ الحاوي على جميع المتجهات التي على الصيغة $(x_1,\ldots,x_{r'},0,\ldots,0,x_{r'+s'+1},\ldots,x_n)$. لكل w في W يكون $(wM,w)\geqslant 0$. لما كان لـ T معكوس ولأن بعد W يساوي $n-s'$ فإن بعد WT يساوي $n-s'$. لكل w في W يكون

$(wM,w)\geqslant 0$ وعليه $(wTLT',w)\geqslant 0$ أي $(wTL,wT)\geqslant 0$. إذن على WT يكون $(wTL,wT)\geqslant 0$ لجميع العناصر. الآن:

$$\dim (WT)+\dim U=(n-s')+s=n+s-s'>n$$

لذا $WT\cap U\neq 0$ استنادا لنتيجة تمهيدية (٤-٢-٦). بيد أن هذا خطأ، لأنه إذا كان $x\neq 0$ في $WT\cap V$ فإنه لكونه في U يكون $(xL,x)<0$. ومن ناحية أخرى يكون $(xL,x)\geqslant 0$ لكونه في WT. لذا $r=r'$ مما يجعل $s=s'$.

إن المرتبة $r+s$ والتوقيع $r-s$ يحددان بالطبع r و s وكذلك $t=n-r-s$ ، لذا فإنهما يحددان فصل التطابق.

مسائل

١ - عين مرتبة وتوقيع الصيغتين التربيعيتين الحقيقيتين التاليتين:

(ا) $x_1^2+2x_1x_2+x_2^2$.

(ب) $x_1^2+x_1x_2+2x_1x_3+2x_2^2+4x_2x_3+2x_3^2$.

٢ - إذا كانت A مصفوفة متناظرة عناصرها أعداد مركبة. فبرهن على أنه توجد مصفوفة B لها معكوس وعناصرها أعداد مركبة $BAB'=\begin{pmatrix} I_r & \\ & 0 \end{pmatrix}$ وأن r الذي يساوي مرتبة A يحدد فصل تطابق A بالنسبة إلى التطابق على حقل الأعداد المركبة.

٣ - إذا كان F حقلاً مميزه لا يساوي 2. فأثبت أنه لكل A في F_n يوجد B في F_n بحيث تكون BAB' مصفوفة قطرية.

٤ - برهن على أن نتيجة مسألة (٣) تكون غير صحيحة إذا كان مميز F يساوي 2.

٥ - كم عدد فصول التطابق للمصفوفات الحقيقية المتناظرة من نوع $n\times n$ ؟

قراءة إضافية

Halmos, Paul R., *Finite-Dimensional Vector Spaces, 2nd Ed.* Princeton, N.J.: D. Van Nostrand Company, 1958.



مواضيع مختارة

● الحقول المنتهية ● مبرهنة فدربرن ● حلقات القسمة المنتهية ● إحدى مبرهنات فروبينيس ● الرباعيات التامة ومبرهنة المربعات الأربعة.

لقد وضعنا هدفين لهذا الفصل: **أولهما** تقديم بعض النتائج الرياضية التي تتصف بعمق أكثر من أغلب المواضيع التي درسناها حتى الآن ـ إن هذه النتائج أكثر تطورا من سابقاتها وهي في الوقت نفسه بعيدة بعض الشيء عن مجرى العرض الذي نهجناه حتى الآن. إن هدفنا **الثاني** هو اختيار نتائج تستدعي دراستها معرفة العديد من الأفكار والمبرهنات التي قدمناها سابقًا في هذا الكتاب. على هذا الأساس قررنا اختيار ثلاثة مواضيع لتصبح بؤرة دراستنا في هذا الفصل.

إن أول هذه المواضيع هي المبرهنة المشهورة للرياضي فدربرن (Wedderburn) التي برهنها عام ١٩٠٥ (مبرهنة «الجبر» المنتهي).

(**A Theorem on Finite Algebras,** Transactions of the American Mathematical Society, Vol. 6 (1905), 349-352).

وهذه المبرهنة تنص على أن حلقة القسمة التي تحوي عددًا منتهيًا من العناصر لابد وأن تكون حقلاً إبداليًّا. سوف نقدم برهانين لهذه المبرهنة يختلفان تماما عن بعضهما، **البرهان الأول** سيكون قريبًا من برهان فدربرن الأصلي وسنستعمل به طريقة العد. إنه سيعتمد بصورة كبيرة على النتائج التي طوّرناها في الفصل الخاص بنظرية الزمر، أما **البرهان الثاني** فإنه سيكون خليطًا من أفكار في نظرية الزمر ونظرية الحقول وسيعتمد

بشكل واضح على المادة المطوّرة في هذا الكتاب في كلا الموضوعين. يتميز البرهان الثاني بأنه يعطينا نتائج جانبية سوف تمكننا من برهان مبرهنة جميلة في حالة حلقات القسمة تعود للرياضي **جيكوبسن** (Jacobson) (دراسة بنيوية للجبر ذي الدرجة المحدودة).
(**Structure Theory for Algebraic Algebra of Bounded Degree,** Annals of Mathematics, Vol. 46 (1945), 695-707).
ومبرهنة **جيكوبسن** تعتبر تعميمًا واسعًا جدًّا لمبرهنة فردبرن.

إن موضـوعنـا الثـاني هو مبرهنة تعود للرياضي **فروبينيس** (Frobenius) (عن التحويلات الخطية والصيغ الخطية الثنائية)
(**"Uber lineare Substitutionen und bilineare Formen",** *Journal für die Riene und Angewandte Mathematik,* 84 (1877), 56-63).
وتنص هذه المبرهنة على أن حلقات القسمة الجبرية على حقل الأعداد الحقيقية هي فقط حقل الأعداد الحقيقية وحقل الأعداد المركبة وحلقة الرباعيات الحقيقية. إن المبرهنة تشير إلى الدور الرئيس للرباعيات وتجعل من المدهش أن يتمكن العالم **هاملتون** من اكتشافها بطريقة ارتجالية. إن برهاننا الذي سنقدمه لمبرهنة **فروبينيس** سيكون ابتدائيًّا وهـو تغيير بسيط عن نهج كل من **دكسن** (Dickson) **وألبـرت** (Albert). إن البرهان سيشتمل على أفكار من نظرية كثيرات الحدود والحقول.

أما هدفنا **الثالث** فهو المبرهنة التي تنص على أنه يمكن تمثيل كل عدد صحيح موجب كحاصل جمع أربعة مربعات. إن هذه النتيجة المشهورة تعود إلى عهد الإغريق حيث كانت حدسًـا للعـالم الإغـريقي **دايـوفانتوس** (Diophantos). لقد حاول **فرما** (Fermat) برهـانها بيد أنه عجز عن ذلك (وذكر هذا في بحث برهن فيه على مبرهنة المربعين التي أثبتناها في بند ٣ـ٨). أما الرياضي **أويلر** (Euler) فقد حقق تقدمًا في الحصول على البرهان. لكن أول من برهنها هو الرياضي **لاجرانج** (Lagrange) في عام ١٧٧٠ مستفيدًا مما وصـل إليه **أويلر**. إن طريقنـا ستكـون مختلفـة تماما عن طريقة لاجـرانـج وهي تعود لعمل العالم الرياضي **هرفتس** (Hurwitz) وتحوي تعميمًا لفكرة

الحلقات الإقليدية. باستخدام طرق نظرية الحلقات في حلقة معيّنة من الرباعيات، سنحصل على مبرهنة لاجرانج كنتيجة مباشرة من ذلك.

في طريقنا لإثبات هذه النظريات سنتطرق للعديد من الأفكار ونحصل على نتائج شيّقة بحد ذاتها. إن هذا ما يميز المبرهنة الجيدة بأن برهانها يقودنا عادة إلى نتائج جانبية ذات أهمية تضاهي أهمية المبرهنة نفسها.

(٧-١) الحقول المنتهية

قبل الدخول في نقاش مبرهنة فدربرن وحلقات القسمة المنتهية، من الضروري أن ندرس طبيعة الحقول التي تحوي عددًا منتهيًا من العناصر. تُدعى مثل هذه الحقول **بالحقـول المنتهية** (finite fields) إن الحقول المنتهية موجودة ومثال على ذلك Z_p حقل الأعداد الصحيحة قياس أي عدد أولي p. في هذا البند سوف نعين جميع الحقول المنتهية بالإضافة إلى العديد من الخواص المهمة التي تتمتع بها.

نبدأ بالتمهيدية التالية.

تمهيدية (٧-١-١)

ليكن F حقلاً منتهيًا يحوي q من العناصر وافرض أن $F\subset K$ حيث K حقل منته أيضًا. عندئذ K يحوي q^n من العناصر حيث $n=[K:F]$.

البرهان

إن K فضاء متجهات على F ولكونه منتهيًا فيجب أن يكون منته البعد كفضاء متجهات على F. افرض أن $[K:F]=n$ ، لذا يكون لـ K أساس على F يحوي n من العناصر ولنفرض أن $v_1,v_2,\ldots,v_n$ هو أساس K على F. إذن أي عنصر في K له تمثيل وحيد على الشكل $\alpha_1v_1+\alpha_2v_2+\ldots+\alpha_nv_n$ حيث $\alpha_1,\alpha_2,\ldots,\alpha_n$ في F. لذا فإن عدد عناصر K هو عدد العناصر التي على الصيغة $\alpha_1v_1+\alpha_2v_2+\ldots+\alpha_nv_n$ حيث مجال تغيير $\alpha_1,\alpha_2,\ldots,\alpha_n$ هو F. بما أن كل معامل يمكن أن يأخذ q من القيم فنستنتج من ذلك أن K يحوي q^n من العناصر.

نتيجة (١)

إذا كان F حقلًا منتهيًا فإن عـدد عنـاصر F هو p^m حيث إن العدد الأولي p هو مميز F.

البرهان

لما كان عدد عناصر F منتهيًا فوفقًا لنتيجة (٢) من مبرهنة (٢-٤-١) يكون $f1=0$ حيث f عدد عناصر F. لذا فإن مميز F يساوي p حيث p عدد أولي. إذن F يحوي حقلاً F_0 يمـاثل Z_p. لما كان عدد عناصر F_0 هو p فإن عدد عناصر F هو p^m حيث $m=[F:F_0]$ استنادًا إلى تمهيدية (٧-١-١).

نتيجة (٢)

إذا كان عدد عناصر الحقل المنتهي يساوي p^m فإنه لأي a في F يكون $a^{p^m}=a$

البرهان

إذا كان $a=0$ فإن ما تزعمه النتيجة صحيح حتمًا.

من ناحية أخـرى فإن العناصر غير الصفرية في F تكون زمرة بالنسبة لعملية الضرب رتبتها p^m-1 ، لذا فوفقًا لنتيجة (٢) من مبرهنة (٢-٤-١) يكون $a^{p^m-1}=1$ لكل $a\neq0$ في F. بضرب هذه العلاقة بالعنصر a نحصل على $a^{p^m}=a$.

من هذه النتيجة الأخيرة يمكننا أن نتجه إلى التمهيدية التالية.

تمهيدية (٧-١-٢)

إذا كان عدد عناصر الحقل المنتهي هو p^m فإن كثـيرة الحدود $x^{p^m}-x$ في $F[x]$ تتحلل في $F[x]$ على النحو

$$x^{p^m}-x=\Pi_{\lambda\in F}(x-\lambda)$$

البرهان

باستخدام تمهيدية (٥-٣-٢) فإن عدد جذور كثير الحدود $x^{p^m}-x$ في F لا يزيد عن p^m. ولكن وفقا لنتيجة (٢) من تمهيدية (٧-١-١) هناك p^m من الجذور في F وهي جميع عناصر F. من نتيجة تمهيدية (٥-٣-١) نستنتج أن $x^{p^m}-x=\Pi_{\lambda\in F}(x-\lambda)$

نتيجة

إذا كان عدد عناصر F هو p^m فإن F هو حقل انشطار كثيرة الحدود $x^{p^m}-x$.

البرهان

استنادا لتمهيدية (٧-١-٢) فإن $x^{p^m}-x$ تنشطر في F. ولكن $x^{p^m}-x$ لا يمكن أن تنشطر في أي حقل أصغر من ذلك لأن مثل هذا الحقل يجب أن يحوي جميع جذور كثيرة الحدود هذه وعليه فإنه يحتوي على ما لا يقل عن p^m من العناصر. لذا فإن F هو حقل انشطار $x^{p^m}-x$.

كما رأينا في الفصل الخامس (مبرهنة ٥-٣-٤) فإن أي حقلي انشطار لكثيرة حدود على حقل معيّن متماثلان. على ضوء نتيجة تمهيدية (٧-١-٢) يمكننا أن نكتب.

تمهيدية (٧-١-٣)

الحقلان المنتهيان الحاويان على العدد نفسه من العناصر متماثلان.

البرهان

إذا كان عدد العناصر في الحقلين هو p^m فاستنادا إلى النتيجة أعلاه يكون كل منهما حقل انشطار لكثيرة الحدود $x^{p^m}-x$ على Z_p لذا فإنهما متماثلان.

لذا فإنه لكل عدد صحيح موجب m وكل عدد أولي p يوجد على الأكثر حقل واحد يحوي p^m من العناصر وذلك إلى حد علاقة التماثل. إن غاية التمهيدية التالية هي إثبات أن لكل عدد أولي p وكل عدد صحيح موجب m يوجد حقل يحوي p^m من

العناصر. عند الانتهاء من هذا فإننا سنعرف أنه يوجد حقل واحد بالضبط يحوي p^m من العناصر حيث p أي عدد أولي و m أي عدد صحيح موجب.

تمهيدية (٧-١-٤)

لكل عدد أولي p وكل عدد صحيح موجب m يوجد حقل يحوي p^m من العناصر.

البرهان

لنعتبر كثيرة الحدود $x^{p^m}-x$ في $Z_p[x]$ وهي حلقة كثيرات الحدود في x على Z_p حقل الأعداد الصحيحة قياس p. ليكن K حقل انشطار كثير الحدود هذه. في K دع $F=\{a\in K|a^{p^m}=a\}$.

إن عناصر F هي جذور $x^{p^m}-x$ والتي هي مختلفة وفقًا لنتيجة (٢) من تمهيدية (٥-٥-٢)، لذا فإن F يحوي p^m من العناصر. إننا ندعي أن F حقل لأنه إذا كان a و b في F فإن $a^{p^m}=a$ و $b^{p^m}=b$ وعليه $(ab)^{p^m}=a^{p^m}b^{p^m}=ab$ مما يجعل ab في F. كذلك لما كان مميز F يساوي p فإن

$$(a\pm b)^{p^m}=a^{p^m}\pm b^{p^m}=a\pm b$$

وعليه يكون $a\pm b$ في F. نستنتج أن F حقل جزئي من K أي أنه حقل. بيد أن F حقل يحوي p^m من العناصر نكون قد برهنا تمهيدية (٧-١-٤).

بالجمع بين التمهيديتين (٧-١-٣) و(٧-١-٤) نحصل على:

مبرهنة (٧-١-١)

لكل عدد أولي p وكل عدد صحيح موجب m يوجد حقل وحيد يحوي p^m من العناصر.

الآن نعود لبعض الوقت إلى نظرية الزمر. إن النتيجة التي ننشدها من نظرية الـزُّمَر تحدد بناء أية زمرة جزئية من زمرة العناصر غير الصفرية في أي حقل بالنسبة لعملية الضرب، وعلى وجه الخصوص فإنها تحدد البناء الضربي لأي حقل منتهي.

تمهيدية (٧-١-٥)

لتكن G زمرة إبدالية منتهية فيها تتحقق العلاقة $x^n=e$ لعدد من العناصر لا يزيد عن n وذلك لكل عدد صحيح موجب n. عندئذ فإن G زمرة دورية.

البرهان

إذا كانت رتبة G هي قوة لعدد أولي q فإن التمهيدية سهلة جدًا. فلو كان a في G عنصرًا رتبته أكبر ما يمكن فإن هذه الرتبة يجب أن تكون q^r لعدد صحيح موجب r. إن العناصر $e,a,a^2,\dots,a^{q^r-1}$ تعطينا q^r من الحلول المختلفة للمعادلة $x^{q^r}=e$ وحسب فرضيتنا تكون هذه العناصر هي جميع حلول تلك المعادلة. الآن إذا كانت رتبة b في G هي q^s حيث $s\leq r$ فإن $b^{q^r}=(b^{q^s})^{q^{r-s}}=e$. مما ذكرناه أعلاه فإن هذا يجعل $b=a^i$ لعدد ما i مما يجعل G دورية.

بالنسبة للزمرة الإبدالية العامة G فيمكن النظر إليها على النحو $G=S_{q_1}S_{q_2}\dots S_{q_k}$ حيث q_i هي القواسم الأولية المختلفة لـ $0(G)$ وحيث S_{q_i} هي زمر سيلو الجزئية في G. بالإضافة إلى ذلك فإن كل عنصر g في G يمكن أن يكتب بطريقة وحيدة على الصيغة $g=s_1s_2\dots s_k$ حيث s_i في S_{q_i} (انظر بند ٢-٧). إن كل حل لـ $x^n=e$ في S_{q_i} هو حل لذات المعادلة في G لذا فإن فرضيتنا على G تنطبق على S_{q_i}. باستخدام الملاحظات في الفقرة الأولى من البرهان فإن كل S_{q_i} هي زمرة دورية مولدة بعنصر نرمز له بـ a_i. إننا ندّعي أن $c=a_1a_2\dots a_k$ يولد G ومن أجل التحقق من ذلك، كل ما علينا أن نفعله هو بيان أن $0(G)$ يقسم رتبة c والتي نرمز لها بـ m. لما كان $c^m=e$ فإن $a_1{}^m a_2{}^m\dots a_k{}^m=e$. باستخدام وحدانية تمثيل عناصر G كحاصل ضرب لعناصر في S_{q_i} نستنتج أن $a_i{}^m=e$. لذا فإن $0(S_{q_i})|m$ لكل i. إذن

$$0(G)=0(S_{q_1})0(S_{q_2})\dots 0(S_{q_k})|m$$

ولكن $m|0(G)$ لذا $0(G)=m$. وهذا يبرهن على أن G زمرة دورية.

إن لتمهيدية (٧-١-٥) استنتاج مهم هو التمهيدية التالية.

تمهيدية (٧-١-٦)

ليكن K حقلاً و G زمرة جزئية منتهية من زمرة العناصر غير الصفرية في K بالنسبة لعملية الضرب عندئذ فإن G زمرة دورية.

البرهان

لما كان K حقلاً فإن عدد الجذور في K لكثيرة حدود من الدرجة n في K[x] لا يزيد عن n. لذا وعلى وجه الخصوص لا يزيد عدد جذور كثيرة الحدود x^n-1 في K عن n. لكل عدد صحيح موجب n مما يجعل ذات الشيء ينطبق على G حتما. بهذا تكون فرضية تمهيدية (٧-١-٥) قد تحققت فنستنتج أن G دورية.

بالرغم من كون حالة الحقل المنتهي مجرد حالة خاصة من تمهيدية (٧-١-٦) فإننا نفردها بسبب أهميتها.

مبرهنة (٧-١-٢)

زمرة العناصر غير الصفرية في حقل منته بالنسبة لعملية الضرب هي زمرة دورية.

البرهان

ليكن F حقلاً منتهيًا. بمجرد تطبيق تمهيدية (٧-١-٦) على F=K و G زمرة العناصر غير الصفرية في F ، نحصل على المبرهنة.

نختم هذا البند باستخدام طرق عد نبرهن منها على وجود حلول لمعادلات معيّنة في الحقل المنتهي. سوف نحتاج هذا في أحد برهانيْ مبرهنة فدربرن.

تمهيدية (٧-١-٧)

ليكن F حقلاً منتهيًا و $\alpha\neq0$ و $\beta\neq0$ عنصرين في F عندئذ يوجد عنصران a و b في F بحيث $1+\alpha a^2+\beta b^2=0$.

البرهان

إذا كان مميز F يساوي 2 فإن عدد عناصر F يساوي 2^n وأي عنصر x في F يحقق $x^{2^n} = x$. لذا فإن كل عنصر في F هو مربع لعنصر آخر. وعلى وجه الخصوص $\alpha^{-1}=a^2$ لعنصر a في F. باستخدام هذا العنصر a و b=0 نحصل على

$$1+\alpha a^2+\beta b^2=1+\alpha\alpha^{-1}+0=1+1=0$$

حيث إن المتساوية الأخيرة هي نتيجة لكون مميز F يساوي 2.

إذا كان مميز F يساوي p حيث p عدد أولي فردي ، فإن عدد عناصر F يساوي p^n.

دع

$$W_\alpha=\{1+\alpha x^2|x\in F\}$$

كم عدد عناصر W_α ؟ **يجب علينا أن نحسب عدد المرات التي فيها** $1+\alpha x^2=1+\alpha y^2$. **ولكن هذه العلاقة تجعل** $\alpha x^2=\alpha y^2$ **مما يقتضي أن يكون** $x^2=y^2$ **لأن** $\alpha\neq0$. **إن هذا يقودنا إلى أن** $x=\pm y$. لذا فلكل $x\neq0$ **نحصل من كل زوج x و x- على عنصر واحد في** W_α ، **ولـ** $x=0$ **نحصل على أن 1 في** W_α. **إذن عدد عناصر** W_α **هو**

$$.1+(p^n-1)/2=(p^n+1)/2$$

بصورة مشابهة نستنتج أن عدد عناصر $W_\beta=\{-\beta x^2|x\in F\}$ **هو** $(p^n+1)/2$. **لما كان عدد العناصر في كل من** W_α **و** W_β **يزيد على نصف عدد العناصر في F فلابد أن يكون تقاطعهما غير خال.** ليكن c في $W_\alpha\cap W_\beta$. **لما كان c في** W_α **فإن** $c=1+\alpha a^2$ **لعنصر ما a في F. ولكون c في** W_β **فإن** $c=-\beta b^2$ **لعنصر ما b في F. إذن** $1+\alpha a^2=-\beta b^2$ **أي** $1+\alpha a^2+\beta b^2=0$ **بعد نقل الحد الأيمن إلى جهة اليسار.**

مسائل

١ - وفقا لمبرهنة (٧-١-٢) فإن العناصر غير الصفرية في Z_p تكون زمرة دورية بالنسبة لعملية الضرب. إن أي مولد لهذه الزمرة يدعى **جذرًا بدائيًّا** (primitive root) لـ p

(ا) أوجد جذورا بدائية لـ: 17, 23, 31

(ب) كم عدد الجذور البدائية لعدد أولي p.

٢ ـ باستخدام مبرهنة (٧ـ١ـ٢) أثبت أن $x^2 \equiv -1$ قياس p قابلة للحل إذا وفقط إذا كان العدد الأولي الفردي p على الصيغة $4n+1$.

٣ ـ إذا كان a عددًا صحيحًا لا يقبل القسمة على العدد الأولي الفردي p. فبرهن على أن $x^2 \equiv a$ قياس p قابلة للحل لعدد صحيح x إذا وفقط إذا كان $a^{(p-1)/2} \equiv 1$ قياس p (يسمى هذا **بمعيار أويلر** (Euler criterion) لكون a باقيًا تربيعيًّا قياس p).

٤ ـ باستخدام مسألة ٣ حدد فيما إذا

(ا) كان 3 مربعا قياس 17.

(ب) كان 10 مربعا قياس 13.

٥ ـ إذا كان عدد عناصر الحقل F هو p^n. فبرهن على أن التماثلات الذاتية لـ F تكون زمرة دورية رتبتها n.

٦ ـ إذا كان F حقلا منتهيًا فنعرف الرباعيات على F بأنها مجموعة جميع العناصر على الصيغة $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ حيث $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ في F وحيث إن عمليتي الجمع والضرب تشبهان نظيرتيهما في الرباعيات الحقيقية (أي $i^2=j^2=k^2=ijk=-1$ الخ).
أثبت أن الرباعيات على الحقل المنتهي لا تكوّن حلقة قسمة.

(٧ـ٢) مبرهنة ڤدربرن (Wedderburn)
حول حلقات القسمة المنتهية

في عام ١٩٠٥ برهن ڤدربرن المبرهنة التي تعتبر الآن تقليدية وهي أن أية حلقة قسمة منتهية يجب أن تكون حقلاً إبداليًّا. لقد حازت هذه النتيجة على اهتمام أغلب علماء الرياضيات لأنها غير متوقعة، حيث إنها تربط بين شيئين يبدو أنه لا علاقة بينهما، وهما عدد العناصر في نظام جبري معيّن وعملية الضرب في ذلك النظام. بالإضافة إلى جمالها الجوهري فهذه المبرهنة مهمة جدًّا ومفيدة في الوقت نفسه لأنها تظهر في العديد من المواضع. ومثال على ذلك، فإن البرهان الوحيد المعروف حتى الآن للحقيقة الهندسية المجردة القائلة بأنه في الهندسة المنتهية أن تشكُّل ديزارج (Desargues) يقتضي تشكُّل بابس (Pappus) (لغرض معرفة تعاريف هذه العبارات انظر أي كتاب جيد عن

الهندسة الإسقاطية) يكون بتحويل المسألة الهندسية إلى جبرية وأن المسألة الجبرية تُحَل باستخدام مبرهنة ڤدربرن.

إن مبرهنة ڤدربرن كانت انطلاقة للمشتغلين في علم الجبر في مجال بحثي واسع خلال الأربعينيات والخمسينيات في هذا القرن وذلك فيما يتعلق بإبدالية الحلقات.

مبرهنة (٧-٢-١) ڤدربرن (Wedderburn)

إن كل حلقة قسمة منتهية هي حقل إبدالي.

البرهان الأول

لتكن K حلقة قسمة منتهية ودع

$$Z=\{z\in K|zx=xz \text{ لجميع } x\in K\}$$

يكون المركز. إذا كان عدد عناصر Z هو q فإنه كما في برهان تمهيدية (٧-١-١) يكون عدد عناصر K هو q^n. إن غايتنا هو برهان أن Z=K أو بصورة مكافئة أن n=1.

إذا كان a في K فدع

$$N(a)=\{x\in K|ax=xa\}$$

من الواضح أن N(a) تحوي Z ومن السهل التحقق من أن N(a) حلقة قسمة جزئية في K. لذا فإن N(a) تحوي $q^{n(a)}$ من العناصر حيث n(a) عدد صحيح موجب. إننا ندعي أن $n(a)|n$ وذلك لأن العناصر غير الصفرية في N(a) تكون زمرة جزئية رتبتها $q^{n(a)}-1$ من زمرة العناصر غير الصفرية في K بالنسبة لعملية الضرب والتي عدد عناصرها q^n-1. وفقًا لمبرهنة لاجرانج (مبرهنة ٢-٤-١) فإن $q^{n(a)}-1$ يقسم q^n-1 ، وهذا يجعل n(a) يقسِّم n (انظر مسألة ١ في نهاية هذا البند).

في زمرة العناصر غير الصفرية في K لدينا علاقة الترافق المستعملة في الفصل الثاني وهي أن a يكون مرافقًا لـ b إذا كان $a=x^{-1}bx$ لعنصر $x\neq 0$ في K.

باستخدام مبرهنة (٢ـ١١ـ١) فإن عدد العناصر في K المرافقة لـ a يساوي دليل منظم a في زمرة العناصر غير الصفرية في K.

إذن عدد العناصر المرافقة لـ a في K يساوي $(q^n-1)/(q^{n(a)}-1)$. لاحظ أن a في Z إذا وفقط إذا كان $n(a)=n$ لذا فحَسَب معادلة الفصول (انظر نتيجة مبرهنة ٢ـ١١ـ١) يكون

$$q^n-1=q-1+\sum_{\substack{n(a)|n\\ n(a)\neq n}}\frac{q^n-1}{q^{n(a)}-1} \qquad (١)$$

حيث يتم الجمع لعنصر واحد a في كل فصل ترافق وذلك للعناصر a التي لا تقع في المركز.

إن المسألة أصبحت الآن هي برهان أنه لا توجد معادلة مثل (١) في الأعداد الصحيحة. إلى هذا الحد نكون قد اتبعنا بصورة قريبة البرهان الأصلي لقدربرن. لغرض إثبات استحالة المعادلة (١) استعمل لقدربرن الحقيقة التالية من نظرية الأعداد والعائدة **لبيركهوف وفانديفر** (Birkhoff and Vandiver): إذا كان $n>1$ فإنه يوجِد عدد أولي يقسم q^n-1 ولكنه لا يقسم q^m-1 حيث $m|n$ و $m\neq n$ ما عدا الحالة $2^6-1=63$ الذي عوامله الأولية هي قواسم للعددين 2^2-1 و 2^3-1. والحالة الأخرى عندما $n=2$ و q عدد أولي على الشكل 2^k-1. لو فرضنا صحة هذه النتيجة فكيف ننهي البرهان؟ إن العدد الأولي المذكور أعلاه يقسم الجهة اليسرى من (١) ويقسم كل حد في حاصل الجمع الواقع في الجهة اليمنى لأنه يقسم q^n-1 ولا يقسم $q^{n(a)}-1$. لذا فإن هذا العدد الأولي يقسم $q-1$ وهذا تناقض. بالنسبة للحالة 2^6-1 فإنها تحتاج لبرهان استحالتها ولكن هذا أمر يسير. في حالة $n=2$ التي لا يمكن أن نستعمل فيها الطريقة أعلاه لاحظ أنه لا يمكن أن يوجد حقل جزئي بين Z و K وهذا يجعل $Z=K$ (برهن ذلك ـ انظر مسألة ٢).

ولكننا لا نريد الاعتماد على نتيجة بيركهوف وفانديفر دون برهانها وأن برهانها سيحيد بنا كثيراً عن موضوعنا الرئيس. لذا فلابد أن نبحث عن وسيلة أخرى. إن غايتنا هي إيجاد عدد صحيح يقسم $(q^n-1)/(q^{n(a)}-1)$ لجميع القواسم $n(a)$ للعدد n ما عدا $n(a)=n$ ، ولكنه لا يقسم $q-1$. عندما ننتهي من ذلك ستصبح معادلة (١)

مستحيلة إلا إذا كان $n=1$ مما ينهي برهان مبرهنة ڤدربرن . إن الطريقة التي سنستخدمها تعود إلى نظرية كثيرات الحدود الدورية (لقد ذكرنا كثيرات الحدود هذه في المسائل التي تلت بند ٥-٦) .

لنعتبر كثيرة الحدود x^n-1 كعنصر في $C[x]$ حيث C حقل الأعداد المركبة . في $C[x]$

$$x^n-1=\pi(x-\lambda) \quad (٢)$$

حيث إن حاصل الضرب يشمل جميع الحدود التي فيها $\lambda^n=1$.

يقال عن عدد مركب θ إنه **جذر بدائي للواحد من رتبة** n (primitive nth root of unity) إذا كان $\theta^n=1$ ولكن $\theta^m\neq1$ لكل عدد صحيح موجب $m<n$. إن الأعداد المركبة التي تحقق $x^n=1$ تكون زمرة جزئية منتهية بالنسبة لعملية الضرب على الأعداد المركبة وحسب مبرهنة (٧-١-٢) تكون هذه الزمرة دورية . إن أي مولد لهذه الزمرة الدورية يجب أن يكون جذرا بدائيا للواحد من رتبة n ، لذا فقد برهنا على أن مثل هذه الجذور موجودة . (بطريق أخرى، $\theta=e^{2\pi i/n}$ يعطينا جذرًا بدائيًا للواحد من رتبة n).

دع $\Phi_n(x)=\pi(x-\theta)$ حيث إن حاصل الضرب يشمل جميع الحدود التي فيها جذر بدائي للواحد من رتبة n. تدعى كثيرة الحدود هذه **بكثيرة حدود دورية** (cyclotomic polynomial) الآن نكتب بعض كثيرات الحدود الدورية

$\Phi_1(x)=x-1$ ، $\Phi_2(x)=x+1$ ، $\Phi_3(x)=x^2+x+1$ ، $\Phi_4(x)=x^2+1$ ،

$\Phi_5(x)=x^4+x^3+x^2+x+1$ ، $\Phi_6(x)=x^2-x+1$

لاحظ أن جميع كثيرات الحدود هذه واحدية ومعاملاتها أعداد صحيحة .

إن غايتنا الأولى هي برهان أنه بصورة عامة $\Phi_n(x)$ هي كثيرة حدود واحدية معاملاتها أعداد صحيحة . نعيد تجميع عوامل x^n-1 والمعطاة في (٢) لنحصل على

$$x^n-1=\prod_{d|n}\Phi_d(x) \quad (٣)$$

باستعمال الاستقراء الرياضي نفرض أن $\Phi_d(x)$ هي كثيرة حدود واحدية معاملاتها أعداد صحيحة لكل $d|n$ و $d\neq n$. لذا فإن $x^n-1=\Phi_n(x)g(x)$ حيث $g(x)$ كثيرة حدود واحدية معاملاتها أعداد صحيحة . إذن

$$\Phi_n(x)=\frac{x^n-1}{g(x)}$$

ونستنتج من إجراء عملية التقسيم (أو بحساب المعاملات) أن $\Phi_n(x)$ هي كثيرة حدود واحدية معاملاتها أعداد صحيحة.

الآن ندعي أنه لأي قاسم d للعدد n حيث $d\neq n$

$$\Phi_n(x)\,\Big|\,\frac{x^n-1}{x^d-1}$$

بمعنى أن خارج القسمة هو كثيرة حدود معاملاتها أعداد صحيحة. كي نثبت ذلك نلاحظ أولا أن

$$x^d-1=\prod_{k|d}\Phi_k(x)$$

وحيث إن كل قاسم لـ d هو قاسم لـ n فبإعادة تجميع العوامل في الجهة اليمنى من (٣) نحصل على x^d-1 في تلك الجهة. كما أنه لكون $d<n$ فإن x^d-1 لا يشتمل على $\Phi_n(x)$. إذن

$$x^n-1=\Phi_n(x)(x^d-1)f(x)$$

حيث

$$f(x)=\prod_{\substack{k|n,k\neq n\\ k\nmid d}}\Phi_k(x)$$

مما يجعل معاملات $f(x)$ أعدادًا صحيحة فنستنتج أن

$$\Phi_n(x)\,\Big|\,\frac{x^n-1}{x^d-1}$$

الأمر الذي يعني أن خارج القسمة هو كثيرة حدود معاملاتها أعداد صحيحة. وهذا يبرهن على ادعائنا.

لكل عدد صحيح t يكون $\Phi_n(t)$ عددًا صحيحًا ومما تقدم يكون هذا العدد قاسمًا لـ $(t^n-1)/(t^d-1)$. على وجه الخصوص وبالعودة إلى معادلة (١)

$$\Phi_n(q)\,\Big|\,\frac{q^n-1}{q^{n(a)}-1}$$

و $\Phi_n(q)|(q^n-1)$ ، لذا فمن (١) نرى أن $\Phi_n(q)|(q-1)$. لكننا ندعي أنه إذا كان $n>1$ فإن $|\Phi_n(q)|>q-1$. ذلك لأن $\Phi_n(q)=\Pi(q-\theta)$ حيث إن مجال θ هو جميع الجذور البدائية للواحد من رتبة n و $|q-\theta|>q-1$ لكل جذر للواحد $\theta\neq 1$ (برهن على ذلك). إذن

$$|\Phi_n(q)|=\Pi|q-\theta|>q-1$$

من الواضح أن $\Phi_n(q)$ لا يمكن أن يقسم $q-1$ مما يقودنا إلى تناقض. لذا فيجب أن يكون $n=1$ مما يبرهن صحة مبرهنة فدربرن.

البرهان الثاني:

قبل تفحص حلقات القسمة المنتهية مرة أخرى نبرهن بعض التمهيديات.

تمهيدية (٧-٢-١)

لتكن R حلقة و a في R. إذا كان T_a التطبيق من R إلى نفسها والمعرف بـ $xT_a=xa-ax$ فإن

$$xT_a^{\,m}=xa^m-maxa^{m-1}+\frac{m(m-1)}{2}a^2xa^{m-2}-\frac{m(m-1)(m-2)}{3!}a^3xa^{m-3}+\dots$$

البرهان

ما هي $xT_a^{\,2}$ ؟

$$xT_a^{\,2}=(xT_a)T_a=(xa-ax)T_a=(xa-ax)a-a(xa-ax)=xa^2-2axa+a^2x$$

ماذا عن $xT_a^{\,3}$ ؟

$$xT_a^{\,3}=(xT_a^{\,2})T_a=(xa^2-2axa+a^2x)a-a(xa^2-2axa+a^2x)=xa^3-3axa^2+3a^2xa-a^3x$$

بالاستمرار على هذا النحو أو باستعمال الاستقراء الرياضي نحصل على تمهيدية (٧-٢-١).

نتيجة

إذا كانت R حلقة فيها $px=0$ لكل x في R حيث p عدد أولي، فإن

$$xT_a^{\,p^m}=xa^{p^m}-a^{p^m}x$$

البرهان

استنادًا إلى الصيغة المذكورة في تمهيدية (٧-٢-١)، إذا كان $p=2$ فإن $xT_a{}^2=xa^2-a^2x$ لأن $2axa=0$. لذا فإن

$$xT_a{}^4=(xa^2-a^2x)\,a^2-a^2(xa^2-a^2x)=xa^4-a^4x$$

وهكذا بالنسبة لـ $xT_a{}^{2m}$.

إذا كان p عددًا أوليًا فرديًا فباستعمال صيغة تمهيدية (٧-٢-١) مرة أخرى نحصل على

$$xT_a{}^p=xa^p-paxa^{p-1}+\frac{p(p-1)}{2}a^2xa^{p-2}+\ldots-a^px$$

ولما كان

$$p\left|\frac{p(p-1)\ldots(p-i+1)}{i!}\right.$$

لكل $i<p$ ، تصبح جميع الحدود الوسطية صفرًا فنستنتج أن

$$xT_a{}^p=xa^p-a^px=xT_{a^p}$$

الآن

$$xT_a{}^{p^2}=x(T_{a^p})^p=xT_{a^{p^2}}$$

وهكذا بالنسبة للقوى العليا لـ p.

تمهيدية (٧-٢-٢)

لتكن D حلقة قسمة مميزها $p>0$ ومركزها Z وليكن $P=\{0,1,2,\ldots,(p-1)\}$ الحقل الجزئي من Z الذي يماثل Z_p. لنفرض أن $a\in D$ و $a\notin Z$ بحيث $a^{p^n}=a$ لعدد ما $n\geq 1$ ، فإنه يوجد x في D بحيث

١ ـ $xax^{-1}\neq a$

٢ ـ $xax^{-1}\in P(a)$ حيث $P(a)$ هو الحقل الذي نحصل عليه بضم a إلى P.

البرهان

عرف التطبيق T_a من D إلى نفسها بـ $yT_a=ya-ay$ لكل y في D.

إن $P(a)$ حقل منته لأن a جبري على P ولنفرض أن عدد عناصره هو p^m. إن جميع عناصر $P(a)$ تحقق $u^{p^m}=u$. وفقا لنتيجة تمهيدية (٧-٢-١)

$yT_a{}^{p^m}=ya^{p^m}-a^{p^m}y=ya-ay=yT_a$ وهذا يجعل $T_a{}^{p^m}=T_a$.

الآن إذا كان λ في $P(a)$ فإن

$$(\lambda x)T_a=(\lambda x)a-a(\lambda x)=\lambda xa-a\lambda x=\lambda(xa-ax)=\lambda(xT_a)$$

لأن λ يتبادل مع a. لذا فإن التطبيق λI من D إلى نفسها والمعرف بـ $\lambda I:y\rightarrow\lambda y$ يتبادل مع T_a لكل λ في $P(a)$. وفقا لتمهيدية (٧-١-٢) فإن كثيرة الحدود

$$u^{p^m}-u=\prod_{\lambda\in P(a)}(u-\lambda)$$

لما كان T_a يتبادل مع λI لكل λ في $P(a)$ ولكون $T_a{}^{p^m}=T_a$ نحصل على:

$$0=T_a{}^{p^m}-T_a=\prod_{\lambda\in P(a)}(T_a-\lambda I)$$

إذا كان لكل $\lambda\neq 0$ في $P(a)$ لا يفني التطبيق $T_a-\lambda I$ أي عنصر غير صفري في D (إذا كان $y(T_a-\lambda I)=0$ يجعل $y=0$) فلأن $T_a(T_a-\lambda_1 I)\ldots(T_a-\lambda_k I)=0$ حيث $\lambda_1,\ldots,\lambda_k$ عناصر غير صفرية في $P(a)$، نستنتج أن $T_a=0$. أي أن $0=yT_a=ya-ay$ لكل y في D وهذا يجعل a في Z وهو مناقض للفرض. لذا يوجد $\lambda\neq 0$ في $P(a)$ و $x\neq 0$ في D بحيث $x(T_a-\lambda I)=0$. بكتابة هذا بصورة صريحة نحصل على $xa-ax-\lambda x=0$ وعليه يكون $xax^{-1}=a+\lambda\in P(a)$ و $xax^{-1}\neq a$ لأن $\lambda\neq 0$. إن هذا يبرهن التمهيدية.

نتيجــة

في تمهيدية (٧-٢-٢) $xax^{-1}=a^i\neq a$ لعدد صحيح i

البرهان

لتكن رتبة a تساوي s فإنه في الحقل $P(a)$ جميع جذور u^s-1 هي $1,a,a^2,\ldots,a^{s-1}$ لأنها مختلفة عن بعضها وعددها يساوي s. لما كان $(xax^{-1})^s=xa^sx^{-1}=1$ ولكون $xax^{-1}\in P(a)$. فإن xax^{-1} هو جذر في $P(a)$ لـ u^s-1 لذا $xax^{-1}=a^i$.

الآن أصبح لدينا كل ما نحتاجه لتقديم البرهان الثاني لمبرهنة فدربرن.

لتكن D حلقة قسمة منتهية و Z مركزها. بالاستقراء الرياضي يمكننا الفرض أن أية حلقة قسمة يكون عدد عناصرها أقل من عدد عناصر D هي حقل إبدالي.

أولا: نلاحظ أنه إذا كان a و b في D بحيث $b^ta=ab^t$ ولكن $ab\neq ba$ ، فإن $b^t\notin Z$. ذلك لأنه إذا اعتبرنا $N(b^t)=\{x\in D|b^tx=xb^t\}$ فإن $N(b^t)$ حلقة قسمة جزئية في D. فإذا لم تكن $N(b^t)=D$ فحسب فرضية الاستقراء يجب أن تكون إبدالية. ولكن كلًا من a و b في $N(b^t)$ وهما لا يتبادلان. نستنتج أن $N(b^t)$ غير إبدالية مما يجعلها مساوية لـ D ولذا $b^t\in Z$.

إن رتبة كل عنصر غير صفري في D منتهية، لذا فإن إحدى قوى العنصر تقع في Z. إذا كان w في D فنعرف رتبة w بالنسبة إلى Z بأنها أصغر عدد صحيح موجب m(w) بحيث $w^{m(w)}\in Z$. اختر عنصرًا في D وليس في Z بحيث إن رتبته بالنسبة إلى Z هي أصغر ما يمكن ولنرمز لهذه الرتبة بـ r. إننا ندعي أن r عدد أولي ذلك لأنه لو كان $r=r_1r_2$ حيث $1<r_1<r$ فإن a^{r_1} لا يقع في Z. بينما $(a^{r_1})^{r_2}=a^r\in Z$ وهذا يعني أن رتبة a^{r_1} بالنسبة إلى Z أصغر من نظيرتها لـ a. وفقا لنتيجة تمهيدية (٧-٢-٢) يوجد x في D بحيث $xax^{-1}=a^i\neq a$ لذا

$$x^2ax^{-2}=x(xax^{-1})x^{-1}=xa^ix^{-1}=(xax^{-1})^i=(a^i)^i=a^{i^2}$$

بصورة مشابهة نحصل على $x^{r-1}ax^{-(r-1)}=a^{i^{r-1}}$. ولكن r عدد أولي وعليه، فاستنادًا إلى مبرهنة فرما الصغرى (نتيجة ٢-٤-١) يكون $i^{r-1}=1+u_0r$ مما يجعل $a^{i^{r-1}}=a^{1+u_0r}=aa^{u_0r}=\lambda a$ حيث $\lambda=a^{u_0r}$ في Z لذا $x^{r-1}a=\lambda ax^{r-1}$. لما كان $x\notin Z$ فمن طبيعة اختيارنا لـ r، $x^{r-1}\notin Z$ وفقًا للملاحظة في الفقرة أعلاه، لما كان $xa\neq ax$ فإن $x^{r-1}a\neq ax^{r-1}$ وهذا يجعل $\lambda\neq 1$. دع $b=x^{r-1}$ فيكون $bab^{-1}=\lambda a$ ونتيجة لذلك

$$\lambda^ra^r=(bab^{-1})^r=ba^rb^{-1}=a^r$$

لأن a^r في Z. إن هذه العلاقة تجعل $\lambda^r=1$.

إننا ندعي أنه إذا كان $y\in D$ فإنه طالما كان $y^r=1$ يجب أن يكون $y=\lambda^i$ لعدد ما i ، ذلك لأنه في *الحقل* Z(y) يوجد على الأكثر r من الجذور لكثيرة الحدود u^r-1. إن

العناصر $1,\lambda,\lambda^2,\ldots,\lambda^{r-1}$ في Z مختلفة عن بعضها لأن رتبة λ هي العدد الأولي r ، وتعطينا هذه العناصر جميع جذور u^r-1 في Z(y) والتي عددها r وهذا يجعل $y=\lambda^i$.

لما كان $\lambda^r=1$ فإن $b^r=\lambda^r b^r=(\lambda b)^r=(a^{-1}ba)^r=a^{-1}b^r a$ وهذا يجعل $ab^r=b^r a$. لما كان a يتبادل مع b^r ولا يتبادل مع b فمن الملاحظة أعلاه يجب أن يكون b^r في Z. وفقا لمبرهنة (٧-١-٢) تكون زمرة العناصر غير الصفرية في Z بالنسبة لعملية الضرب زمرة دورية. ليكن γ في Z مولدا لهذه الزمرة. لذا $a^r=\gamma^j$ ، $b^r=\gamma^k$. إذا كان j=sr فإن $a^r=\gamma^{sr}$ وعليه $(a/\gamma^s)^r=1$. إن هذا يقتضي أن يكون $a/\gamma^s=\lambda^i$ مما يجعل a في Z وهو مناقض لكون $a\notin Z$. إذن $r\nmid j$. بصورة مشابهة $r\nmid k$. دع $a_1=a^k$ و $b_1=b^j$ إن حسابًا مباشرًا ابتداء بـ $ba=\lambda ab$ يبين أن $a_1b_1=\mu b_1a_1$ حيث $\mu=\lambda^{-jk}\in Z$. لما كان العدد الأولي r والذي هو رتبة λ لا يقسم j أو k فإن $\lambda^{jk}\neq 1$ إذن $\mu\neq 1$. لاحظ أن $\mu^r=1$.

دعنا نرى إلى أين وصلنا. لقد أوجدنا عنصرين a_1 و b_1 بحيث

١ - $a_1=b_1{}^r=\alpha\in Z$

٢ - $a_1b_1=\mu b_1a_1$ حيث $\mu\neq 1$ في Z

٣ - $\mu^r=1$

لنحسب $(a_1{}^{-1}b_1)^r$.

$$(a_1{}^{-1}b_1)^2=a_1{}^{-1}b_1a_1{}^{-1}b_1=a_1{}^{-1}(b_1a_1{}^{-1})b_1=a_1{}^{-1}(\mu a_1{}^{-1}b_1)b_1=\mu a_1{}^{-2}b_1{}^2$$

إذا حسبنا $(a_1{}^{-1}b_1)^3$ نجده مساويا لـ $\mu^{1+2}a_1{}^{-3}b_1{}^3$. بالاستمرار نحصل على

$$(a_1{}^{-1}b_1)^r=\mu^{1+2+\ldots(r-1)}\ a_1{}^{-r}b_1{}^r=\mu^{1+2+\ldots+(r-1)}=\mu^{r(r-1)/2}.$$

إذا كان r عددا أوليا فرديا فلأن $\mu^r=1$ نستنتج أن $\mu^{r(r-1)/2}=1$ وعليه $(a_1{}^{-1}b_1)^r=1$. لما كان هذا حل لـ $y^r=1$ فيكون $a_1{}^{-1}b_1=\lambda^i$ ومنه $b_1=\lambda^i a_1$. ولكن حينئذ $\mu b_1a_1=a_1b_1=b_1a_1$ وهذا يناقض كون $\mu\neq 1$. لذا فإن كان r عددا أوليا فرديا نكون قد برهنا على المبرهنة.

الآن يجب أن نعالج الحالة r=2. في هذه الحالة الخاصة لدينا عنصران a_1 و b_1 في D بحيث $a_1{}^2=b_1{}^2=\alpha\in Z$ و $a_1b_1=\mu b_1a_1$ حيث $\mu^2=1$ و $\mu\neq 1$. لذا $\mu=-1$ و $a_1b_1=-b_1a_1\neq b_1a_1$. نستنتج من ذلك أن مميز D لا يساوي *2*. استنادا لتمهيدية (٧-١-٧) يمكننا إيجاد عنصرين ζ و η في Z بحيث $1+\zeta^2-\alpha\eta^2=0$. لنعتبر

$$(a_1+\zeta b_1+\eta a_1b_1)^2$$

عند حساب ذلك نجد أن

$$(a_1+\zeta b_1+\eta a_1 b_1)^2=\alpha(1+\zeta^2-\alpha\eta^2)=0$$

ولكوننا في حلقة قسمة نحصل على

$$a_1+\zeta b_1+\eta a_1 b_1=0$$

لذا

$$0\neq 2a_1^2=a_1(a_1+\zeta b_1+\eta a_1 b_1)+(a_1+\zeta b_1+\eta a_1 b_1)a_1=0$$

إن هذا التناقض ينهي برهان مبرهنة فدربرن .

هناك بعض المميزات للبرهان الثاني منها أننا يمكن أن نستخدم بعض أجزائه لبرهان نتيجة رائعة لعالم الرياضيات جيكوبسن (Jacobson) وهي

مبرهنة (٧-٢-٢) جيكوبسن (Jacobson)

لتكن D حلقة قسمة بحيث لكل عنصر a فيها يوجد عدد صحيح موجب $n(a)>1$ معتمدًا على a بحيث $a^{n(a)}=a$ عندئذ فإن D حقل إبدالي .

البرهان

إذا كان $a\neq 0$ في D فإن $a^n=a$ و $(2a)^m=2a$ لعددين صحيحين n و m بحيث $n,m>1$. دع $S=(n-1)(m-1)+1$

إن $s>1$ و $a^s=a$ و $(2a)^s=2a$ وذلك بعد إجراء حساب بسيط . ولكن $(2a)^s=2^s a^s=2^s a$ وعليه $2^s a=2a$ ومن هذا نحصل على $(2^s-2)a=0$. لذا فإن مميز D هو $p>0$. إذا كان P هو الحقل الذي يحوي p من العناصر (يماثل Z_p) داخل Z فلأن a جبري على P يكون $P(a)$ حقلاً منتهيًا عدد عناصره p^h لعدد صحيح موجب h لذا فلكون a في $P(a)$ يصبح $a^{p^h}=a$.
إذن إذا كان $a\notin Z$ فإن جميع شروط تمهيدية (٧-٢-٢) متحققة، وعليه يوجد b في D بحيث

$$bab^{-1}=a^{\mu}\neq a \qquad (١)$$

باستخدام الطريقة نفسها $b^{p^k}=b$ لعدد صحيح $k>1$. دع

$$W=\{x\in D \mid x=\sum_{i=1}^{p^h}\sum_{j=1}^{p^k} p_{ij}a^i b^j \text{ حيث } p_{ij}\in P\}$$

إن W مجموعة منتهية مغلقة بالنسبة لعملية الجمع . ومن (١) نرى أن W مغلقة بالنسبة لعملية الضرب . (تحقق من ذلك!) . لذا فإن W حلقة منتهية ولكونها حلقة جزئية من حلقة القسمة D فيجب أن تكون هي نفسها حلقة قسمة (مسألة ٣) . إذن W حلقة قسمة منتهية . وفقًا لمبرهنة فدربرن فإن W إبدالية . ولكن a و b كلاهما في W مما يجعل $ab=ba$ وهذا يناقض كون $a^{\mu}b=ba$ مما يثبت المبرهنة .

إن مبرهنة جيكوبسن في الحقيقة صحيحة *لكل حلقة* R تحقق $a^{n(a)}=a$ لكل a في R وليست مقتصرة على حلقات القسمة . إن الانتقال من حالة حلقة القسمة إلى الحالة العـامة ليس صعبًا ولكنه يتطلب استعمال *مسلمة الاختيار* (axiom of choice) والتي شرحها يخرجنا عن الإطار العام لدراستنا .

مســائــل

١ ـ إذا كان $t>1$ عددًا صحيحًا و $(t^m-1)|(t^n-1)$ ، فبرهن على أن $m|n$.

٢ ـ إذا كانت D حلقة قسمة . فأثبت أن بعدها (كفضاء متجهات) على مركزها لا يمكن أن يساوي 2.

٣ ـ أثبت أن كل حلقة جزئية منتهية من حلقة قسمة هي حلقة قسمة .

٤ ـ (ا) لتكن D حلقة قسمة مميزها $p\neq 0$ ولتكن G زمرة جزئية منتهية من زمرة العناصر غير الصفرية في D بالنسبة لعملية الضرب . أثبت أن G إبدالية .

(ب) في الجزء (ا) برهن على أن G في الحقيقة دورية .

*٥ ـ (ا) إذا كانت R حلقـة منتهية فيهـا $x^n=x$ لكل x في R حيث $n>1$ فبرهن على أن R إبدالية .

(ب) إذا كانت R حلقـة منتهية فيها $x^2=0$ تقتضي أن يكون $x=0$. فأثبت أن R إبدالية .

*٦ ـ لتكن D حلقة قسمة افرض أن a في D له عدد منته من العناصر المترافقة (بمعـنى عدد منته من العناصر المختلفة على الصيغة $x^{-1}ax$). أثبت أن لـ a عنصرًا مترافقًا واحدًا فقط ويجب أن يكون في مركز D.

٧ ـ استعمل نتيجة مسألة (٦) لبرهان أنه إذا كان لكثيرة حدود درجتها n ومعاملاتها في مركز حلقة قسمة n+1 من الجذور في حلقة القسمة، فإن له عددًا غير منته من الجذور في حلقة القسمة تلك.

٨* ـ لتكن D حلقة قسمة و K حلقة قسمة جزئية من D بحيث $xKx^{-1} \subset K$ لكل $x \neq 0$ في D. برهن على أنه إما $K \subset Z$ حيث Z مركز D أو K=D. (تُعرف هذه النتيجة بمبرهنة براور ـ كارتان ـ هوا (Brauer-Cartan-Hua).

٩* ـ لتكن D حلقة قسمة و K حلقة قسمة جزئية. افرض أن زمرة العناصر غير الصفرية في K هي زمرة جزئية ذات دليل منته في زمرة (بالنسبة لعملية الضرب) العناصر غير الصفرية في D. أثبت أنه إما أن تكون D منتهية أو أن K=D.

١٠ ـ إذا كان $\theta \neq 1$ جذرًا للواحد وكان q عددا صحيحا موجبا. فبرهن على أن $|q-\theta| > q-1$.

(٧-٣) إحدى مبرهنات فروبينيس (Frobenius)

في عام ١٨٧٧م صنف العالم الرياضي فروبينيس Frobenius جميع حلقات القسمة التي تحوي حقل الأعداد الحقيقية في مركزها وتحقق شرطًا آخر نذكره أدناه. إن غاية هذا البند هي تقديم نتيجة فروبينيس هذه.

لقد لفتنا الانتباه في الفصل السادس إلى حقيقتين مهمتين عن حقل الأعداد المركبة وهما:

حقيقة (١)

جميع جذور كثيرة الحدود من الدرجة n على حقل الأعداد المركبة تقع في حقل الأعداد المركبة وعددها يساوي n.

حقيقة (٢)

إن كثيرات الحدود غير المختزلة على حقل الأعداد الحقيقية هي إما من الدرجة 1 أو 2.

تعريف

يقال عن جبر قسمة D إنه جبري على الحقل F إذا

١ ـ *كان F محتوى في مركز D.*

٢ ـ *كان كل a في D يحقق كثيرة حدود غير تافهة معاملاتها في F.*

إذا كان D منتهي البعد كفضاء متجهات على الحقل F الذي يوجد داخل مركز D. فمن السهولة إثبات أن D جبري على F (انظر مسألة ١ في نهاية هذا البند). غير أنه من الممكن أن يكون D جبريًا على F دون أن يكون منتهي البعد على F.

نبدأ دراستنا لحلقات القسمة الجبرية على حقل الأعداد الحقيقية بتصنيف حلقات القسمة الجبرية على حقل الأعداد المركبة.

تمهيدية (٧-٣-١)

ليكن C حقل الأعداد المركبة ولنفرض أن حلقة القسمة D جبرية على C. عندئذ $D=C$.

البرهان

لنفرض أن a في D. لما كانت D جبرية على C فإن:

$a^n+\alpha_1a^{n-1}+\ldots+\alpha_{n-1}a+\alpha_n=0$ حيث $\alpha_1,\alpha_2,\ldots,\alpha_n$ في C.

الآن كثيرة الحدود

$p(x)=x^n+\alpha_1x^{n-1}+\ldots+\alpha_{n-1}x+\alpha_n$ في $C[x]$.

إذن استنادا إلى حقيقية (١)، يمكن تحليلها في $C[x]$ إلى حاصل ضرب عوامل خطية أي $p(x)=(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_n)$ حيث $\lambda_1,\lambda_2,\ldots,\lambda_n$ كلها في C. لما كان C في مركز D فإن كل عنصر في C يتبادل مع a لذا $p(a)=(a-\lambda_1)(a-\lambda_2)\ldots(a-\lambda_n)$. ولكن $p(a)=0$ بالفرض، إذن $(a-\lambda_1)(a-\lambda_2)\ldots(a-\lambda_n)=0$. ولما كان حاصل الضرب في حلقة قسمة يساوي صفرًا إذا وفقط إذا كان أحد العوامل يساوي صفرًا، نستنتج أن $a-\lambda_k=0$ لعدد ما $1\leqslant k\leqslant n$

وعليه يكون $a=\lambda_k$ فيكون a في C. إذن كل عنصر في D هو عنصر في C ولكون $C\subset D$ نحصل على أن $C=D$.

نحن الآن في وضع يؤهلنا لبرهان نتيجة فروبينيس التقليدية وهي .

مبرهنة (٧-٣-١) فروبينيس (Frobenius)

لتكن D حلقة قسمة جبرية على حقل الأعداد الحقيقية F . عندئذ D تماثل واحدًا مما يلي: *حقل الأعداد الحقيقية ، حقل الأعداد المركبة أو حلقة الرباعيات الحقيقية .*

البرهان

إن البرهان يشتمل على ثلاثة أجزاء . **في الجزء الأول** وهو الأسهل نثبت المبرهنة في حالة كون D إبدالية . **في الجزء الثاني** نفرض أن D غير إبدالية وتنشىء نموذجا مماثلا للرباعيات الحقيقية في D. **في الجزء الثالث** نبرهن على أن هذا النموذج يملأ جميع الحلقة D.

لنفرض أن $D\neq F$ وأن a في D ولكنه ليس في F. من الفرض نعلم أن a يحقق كثيرة حدود على F ، وعليه فإنه يحقق كثيرة حدود غير مختزلة على F. وفقًا لحقيقة 2 فإن a يحقق إما معادلة خطية أو تربيعية على F. إذا كانت المعادلة خطية يصبح a في F وهو مناقض للفرض. لذا يمكن الفرض أن $a^2-2\alpha a+\beta=0$ حيث α و β في F. لذا $(a-\alpha)^2=\alpha^2-\beta$ ، إننا ندعي أن $\alpha^2-\beta<0$ لأنه لو لم يكن كذلك لكان له جذر تربيعي حقيقي δ ونحصل على $a-\alpha=\pm\delta$ مما يجعل a في F. لما كان $\alpha^2-\beta<0$ فإنه يمكن كتابته على الصيغة $-\gamma^2$ حيث γ في F. إذن $(a-\alpha)^2=-\gamma^2$ وعليه $[(a-\alpha)/\gamma]^2=-1$ نستنتج *أنه إذا كان a في D و $a\notin F$ فيمكن إيجاد عددين حقيقيين α و γ بحيث $[(a-\alpha)/\gamma]^2=-1$.*

إذا كانت D إبدالية فاختر a في D بحيث $a\notin F$ واجعل $i=(a-\alpha)/\gamma$ حيث نختار α و γ في F ليكون $i^2=-1$. إذن D تحوي F(i) وهو حقل يماثل حقل الأعداد المركبة . لما كانت D إبدالية وجبرية على F فإنها حتمًا جبرية على F(i). من تمهيدية (٧-٣-١) نستنتج أن $D=F(i)$. إذن إذا كانت D إبدالية فهي إما F أو F(i).

الآن نفرض أن D غير إبدالية. إننا ندعي أن مركز D يجب أن يساوي F. فإذا لم يكن كذلك فإنه يوجد a في المركز بحيث $a \notin F$. ولكن حينئذ يوجد α و γ في F بحيث $[(a-\alpha)/\gamma]^2=-1$ مما يجعل المركز يحوي حقلاً مماثلاً لحقل الأعداد المركبة. ولكن استنادًا لتمهيدية (٧-٣-١) إذا كان حقل الأعداد المركبة (أو حقل مماثل له) موجودًا داخل مركز D فإن D=C مما يجعل D إبدالية. لذا فإن F يساوي مركز D.

ليكن a في D بحيث $a \notin F$ و $i=(a-\alpha)/\gamma$ حيث α و γ عددان في F بحيث $i^2=-1$.

لما كان $i \notin F$ فإن i ليس في مركز D. لذا فإنه يود عنصر b في D بحيث أن $c=bi-ib \neq 0$.

لنحسب $ic+ci$. $ic+ci=i(bi-ib)+(bi-ib)i=ibi-i^2b+bi^2-ibi=0$ لأن $i^2=-1$ إذن $ic=-ci$. ومن هذا نحصل على $ic^2=-c(ic)=-c(-ci)=c^2i$

لذا فإن c^2 يتبادل مع i. إن c يحقق معادلة تربيعية على F على النحو $c^2+\lambda c+\mu=0$. لما كان c^2 و μ يتبادلان مع i فإن λc يتبادل مع i. أي أن $\lambda ci=i\lambda c=\lambda ic=-\lambda ci$ وعليه $2\lambda ci=0$.

ولكون $2ci \neq 0$ نستنتج أن $\lambda=0$. لذا $c^2=-\mu$. وحيث إن $c \notin F$ (لأن $ci=-ic \neq ic$) يمكننا القول كالسابق إن μ موجب فيكون $\mu=v^2$ حيث $v \in F$. إذن $c^2=-v^2$. دع $j=c/v$ فإن j يحقق

١ - $j^2=\dfrac{c^2}{v^2}=-1$

٢ - $ji+ij=\dfrac{c}{v}i+i\dfrac{c}{v}=\dfrac{ci+ic}{v}=0$

الآن دع $k=ij$. إن العناصر i,j,k التي أنشأناها تحقق خواص مثيلاتها في الرباعيات. لذا $T=\{\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k|\alpha_0,\alpha_1,\alpha_2,\alpha_3 \in F\}$ تكون حلقة قسمة جزئية في D مماثلة للرباعيات الحقيقية. بهذا نكون قد أنشأنا نموذجًا مماثلاً T لحلقة الرباعيات الحقيقية في D.

بقي علينا أن نثبت أن T=D.

إذا كان $r \in D$ يحقق $r^2=-1$ فدع $N(r)=\{x \in D|xr=rx\}$. إن N(r) حلقة قسمة جزئية في D بالإضافة إلى ذلك فإن r وبالأحرى جميع العناصر $\alpha_0+\alpha_1 r$ حيث α_0,α_1 في F تقع في مركز N(r). استنادا إلى تمهيدية (٧-٣-١) فإن $N(r)=\{\alpha_0+\alpha_1 r|\alpha_0,\alpha_1 \in F\}$. لذا إذا كان $xr=rx$ فإن $x=\alpha_0+\alpha_1 r$ حيث α_0,α_1 في F.

لنفرض أن $u \in D$ و $u \notin F$. عندئذ يوجد عنصر $w=(u-\alpha)/\beta$ حيث α و β في F يحقق

$w^2=-1$. إننا ندعي أن $wi+iw$ يتبادل مع كل من i و w. ذلك لأن

$$i(wi+iw)=iwi+i^2w=iwi+wi^2=(iw+wi)i$$

لكون $i^2=-1$ وبصورة مشابهة $w(wi+iw)=(wi+iw)w$. وفقا لملاحظات الفقرة السابقة فإن

$$wi+iw=\alpha_0'+\alpha_1'i=\alpha_0+\alpha_1 w$$

إذا كان $w\notin T$ فإن العلاقة الأخيرة تجعل $\alpha_1=0$ (لأنه خلاف ذلك يمكننا كتابة w بدلالة i). لذا $wi+iw=\alpha_0\in F$. بصورة مشابهة $wj+jw=\beta_0\in F$ و $wk+kw=\gamma_0\in F$. دع

$$z=w+\frac{\alpha_0}{2}i+\frac{\beta_0}{2}j+\frac{\gamma_0}{2}k$$

عندئذ

$$zi+iz=wi+iw+\frac{\alpha_0}{2}(i^2+i^2)+\frac{\beta_0}{2}(ji+ij)+\frac{\gamma_0}{2}(ki+ik)=\alpha_0-\alpha_0=0$$

بصورة مشابهة $zj+jz=0$ و $zk+kz=0$. إننا ندعي أن هذه العلاقات تجعل $z=0$. لأن

$$0=zk+kz=zij+ijz=(zi+iz)j+i(jz-zj)=i(jz-zj)$$

لأن $zi+iz=0$. ولكن $i\neq 0$ ولكوننا في حلقة قسمة نحصل على $jz-zj=0$. غير أن $jz+zj=0$ إذن $2jz=0$ ولما كان $2j\neq 0$ فإننا نستنتج أن $z=0$. بالرجوع إلى تعبير z نحصل على

$$w+\frac{\alpha_0}{2}i+\frac{\beta_0}{2}j+\frac{\gamma_0}{2}k=0$$

مما يجعل $w\in T$ وهذا مناقض لـ $w\notin T$. نستنتج أن w حقا في T. وحيث إن $w=(u-\alpha)/\beta$ فإن $u=\beta w+\alpha$ مما يجعل $u\in T$. لقد برهنا على أن كل عنصر في D هو عنصر في T. وحيث إن $T\subset D$ نستنتج أن $D=T$. ولما كانت T تماثل الرباعيات الحقيقية فنحصل على أن D تماثل حلقة الرباعيات الحقيقية مما ينهي برهان المبرهنة.

مسائل

١ - إذا كانت حلقة القسمة D منتهية البعد كفضاء متجهات على الحقل F الموجود في مركز D. فبرهن على أن D جبرية على F.

٢ ـ أعط مثالاً على حقل K جبري على حقل آخر F ولكنه ليس منتهي البعد على F .

٣ ـ إذا كانت A حلقة جبرية على حقل F وكانت A لا تحوي قواسم للصفر. فبرهن على أن A حلقة قسمة .

(٧ـ٤) الرباعيات التامة ومبرهنة المربعات الأربعة

درسنا في الفصل الثالث نوعًا خاصًا من الحلقات التامة يسمى بالحلقات الإقليدية . عندما طبقنا النتائج التي حصلنا عليها في تلك الحلقات على أعداد جاوس الصحيحة استنتجنا نتيجة **فرما** (Fermat) المشهورة بأن كل عدد أولي على الصيغة 4n+1 هو حاصل جمع مربعين .

أما الآن فسنعتبر حلقة جزئية خاصة من حلقة الرباعيات والتي تشابه في جميع أوجهها الحلقة الإقليدية سوى كونها غير إبدالية . لهذا السبب سيكون من الممكن تمييز جميع مثالياتها اليسرى. إن هذا التمييز للمثاليات اليسرى سيقودنا بسرعة إلى برهان المبرهنة التقليدية للاجرانج والتي تنص على أن كل عدد صحيح موجب هو حاصل جمع أربعة مربعات .

لتكن Q حلقة الرباعيات الحقيقية. في Q نعرف المؤثر القرين * على النحو التالي .

تعريف

*إذا كان $x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ في Q فنعرف **قرين** x(adjoint) ونرمز له بـ x^* على أنه $x^*=\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k$*

تمهيدية (٧ـ٤ـ١)

إن القرين في Q يحقق ما يلي:

١ ـ $x^{**}=x$

٢ ـ $(\delta x+\alpha y)^*=\delta x^*+\gamma y^*$

٣ ـ $(xy)^*=y^*x^*$

لكل x و y في Q وكل الأعداد الحقيقية δ و γ.

البرهان

إذا كان $x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ فإن $x^*=\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k$ وحينئذ $x^{**}=(x^*)^*=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ مما يبرهن الجزء (١).

الآن دع $x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ و $y=\beta_0+\beta_1 i+\beta_2 j+\beta_3 k$ في Q وليكن δ و γ عددين صحيحين اختيارين. عندئذ:

$$\delta x+\gamma y=(\delta\alpha_0+\gamma\beta_0)+(\delta\alpha_1+\gamma\beta_1)i+(\delta\alpha_2+\gamma\beta_2)j+(\delta\alpha_3+\gamma\beta_3)k$$

إذن من تعريف * يكون

$$\begin{aligned}(\delta x+\delta y)^* &= (\delta\alpha_0+\gamma\beta_0)-(\delta\alpha_1+\gamma\beta_1)i-(\delta\alpha_2+\gamma\beta_2)j-(\delta\alpha_3+\gamma\beta_3)k\\ &= \delta(\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k)\ +\gamma(\beta_0-\beta_1 i-\beta_2 j-\beta_3 k)\\ &= \delta x^*+\gamma y^*\end{aligned}$$

وهذا بالطبع يبرهن الجزء (٢).

في ضوء ما أثبتناه في الجزء (٢) فإنه يكفي لبرهان الجزء (٣) أن نثبته لأساس لـ Q على الأعداد الحقيقية، وسنفعل هذا للأساس 1,i,j,k. الآن $ij=k$ لذا

$$(ij)^*=k^*=-k=ji=(-j)(-i)=j^*i^*$$

بصورة مشابهة $(ik)^*=k^*i^*$ و $(jk)^*=k^*j^*$. أيضا $(i^2)^*=(-1)^*=-1=(i^*)^2$ وكذلك بالنسبة لـ k,j. لما كان الجزء (٣) صحيحًا بالنسبة لعناصر الأساس أعلاه ولكون الجزء (٢) صحيحا فإن الجزء (٣) يكون صحيحًا لجميع التركيبات الخطية من عناصر الأساس بمعاملات من الأعداد الحقيقية وعليه يصبح الجزء (٣) صحيحًا لأي عنصرين اختياريين x و y في Q.

تعريف

إذا كان x في Q فنعرّف معيار x (norm) ونرمز له بـ N(x) على النحو $N(x)=xx^*$.

لاحظ أنه إذا كان:

$$x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$$

فإن

$$N(x)=xx^*=(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)(\alpha_0-\alpha_1 i-\alpha_2 j-\alpha_3 k)$$
$$=\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2$$

إذن $N(0)=0$ و $N(x)$ هو عدد حقيقي موجب لكل $x\neq 0$ في Q. على وجه الخصوص، لكل عدد حقيقي α يكون $N(\alpha)=\alpha^2$. إذا كان $x\neq 0$ فلاحظ أن $x^{-1}=(1/N(x))x^*$.

تمهيدية (٧-٤-٢)

لكل x و y في Q ، $N(xy)=N(x)N(y)$

البرهان

من تعريف المعيار فإن $N(xy)=(xy)(xy)^*$. من الجزء (٣) من تمهيدية (٧-٤-١)، $(xy)^*=y^*x^*$ وعليه $N(xy)=xyy^*x^*$. ولكن $yy^*=N(y)$ وهو عدد حقيقي مما يجعله في مركز Q. على وجه الخصوص هذا العدد يتبادل مع x^*. نستنتج أن

$$N(xy)=x(yy^*)x^*=(xx^*)(yy^*)=N(x)N(y)$$

كاستنتاج مباشر من تمهيدية (٧-٤-٢) نحصل على ما يلي.

تمهيدية (٧-٤-٣) متطابقة لاجرانج Lagrange identity

إذا كانت $\alpha_0,\alpha_1,\alpha_2,\alpha_3$ *و* $\beta_0,\beta_1,\beta_2,\beta_3$ *أعدادًا حقيقية فإن*

$$(\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2)\ (\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2)=(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)^2$$
$$+(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)^2+(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)^2$$
$$+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_2\beta_1+\alpha_3\beta_0)^2$$

البرهان

بالطبع يوجد برهان واضح لهذه النتيجة وهو أن نفتح الأقواس ونقارن الحدود.

ولكن ثمة طريقة أبسط من ذلك من ناحية أنها تنشىء المتطابقة وفي الوقت نفسه نبرهنها وذلك بملاحظة أن الجهة اليسرى هي $N(x)N(y)$ بينما الجهة اليمنى هي

N(xy) حيث $x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ و $y=\beta_0+\beta_1 i+\beta_2 j+\beta_3 k$. من تمهيدية (٧-٤-٢) $N(x)N(y)=N(xy)$ مما يبرهن متطابقة لاجرانج .

إن متطابقة لاجرانج تنص على أن حاصل ضرب مجموع أربعة مربعات مع مجموع أربعة مربعات هو بطريقة محددة مجموع أربعة مربعات . هناك نتيجة غريبة لـ **أدلف هرفتز** (Adolf Hurwitz) تنص على أنـه إذا كان حاصل ضرب مجموع n من المربعات بمجموع n من المربعات هو أيضا مجموع n من المربعات بحيث أن حدود المجموع الأخيرة حُسبت بطريقة خطية ثنائية من حدود المجموعين الآخرين فإن n تساوي 1 ، 2 ، 4 أو 8. في الحقيقة توجد متطابقة لحاصل ضرب مجموعي ثمانية مربعات ولكننا لن نكتبها هنا لأنها مطوّلة وشائكة .

والآن فقد حان الوقت المناسب لتقديم حلقة هرفتز للرباعيات التامة .

دع $\zeta=\frac{1}{2}(1+i+j+k)$ ودع

$$H=\{m_0\zeta+m_1 i+m_2 j+m_3 k \mid m_0,m_1,m_2,m_3 \text{ أعداد صحيحة}\}$$

تمهيدية (٧-٤-٤)

*إن H حلقـة جزئية من Q. إذا كان x في H فإن *x في H و N(x) عدد صحيح موجب لكل عنصر $x\neq 0$ في H.*

نترك برهان تمهيدية (٧-٤-٤) للقارىء إذ أننا لا نعتقد أنه يشكل صعوبة عليه .

قد تبدو الحلقة H لأول وهلة أنها مبتدعة . فلماذا نستخدم الرباعي ζ ؟ لماذا لا تعتبر الحلقة الأكثر ألفة Q_0 حيث

$$Q_0=\{m_0+m_1 i+m_2 j+m_3 k \mid m_0,m_1,m_2,m_3 \text{ أعداد صحيحة}\} ؟$$

إن الجواب على ذلك أن Q_0 ليست كبيرة بالحد الكافي على النقيض من H وذلك لفرض أن تكـون التمهيدية التـالية صحيحة . ولكننا نحتاج إلى أن تكون التمهيدية التالية صحيحة في الحلقة التي نتعامل معها لأنها تجعلنا نميز مثالياتها اليسرى . وهذا قد يوضح السبب الذي جعلنا (أو بالأحرى هرفتز) نختار العمل في الحلقة H بدلاً من Q_0.

تمهيدية (٧-٤-٥) خوارزم القسمة الأيسر (Left-division algorhithm)

ليكن a و b عنصرين في H حيث $b\neq 0$. فإنه يوجد عنصران c و d في H بحيث $a=cb+d$ و $N(d)<N(b)$.

البرهان

قبل برهان التمهيدية لننظر إلى ما تخبرنا عنه. إذا رجعنا إلى بند الفصل الثالث المتعلق بالحلقات الإقليدية يمكننا أن نستنتج أن تمهيدية (٧-٤-٥) تؤكد وجود جميع خواص الحلقات الإقليدية في H ما عدا الإبدالية. إن حقيقة كون H غير إبدالية لا تشكل عائقا لنا، ولكن يجب أن نكون حذرين كي لا نخرج باستنتاجات خاطئة، على سبيل المثال $a=cb+d$ ولكن لا يحق لنا الفرض أن $a=bc+d$ لأنه قد لا يتبادل b مع c. لكن هذا سوف لا يؤثر على أية مناقشة أدناه.

لغرض برهان التمهيدية فإننا نثبت أولاً حالة خاصة جدًا وهي التي فيها a عنصر اختياري في H ولكن b عدد صحيح موجب n. لنفرض أن $a=t_0\zeta+t_1i+t_2j+t_3k$ حيث t_0,t_1,t_2,t_3 أعداد صحيحة و $b=n$ حيث n عدد صحيح موجب. دع $c=x_0\zeta+x_1i+x_2j+x_3k$ حيث x_0,x_1,x_2,x_3 أعداد صحيحة تُعيَّن أدناه. إننا نريد اختيار هذه الأعداد بحيث يكون $N(a-cn)<N(n)=n^2$. ولكن

$$a-cn=(t_0(\frac{1+i+j+k)}{2}) +t_1i+t_2j+t_3k)-nx_0(\frac{1+i+j+k}{2})-nx_1i-nx_2j-nx_3k$$

$$=\frac{1}{2}(t_0-nx_0)+\frac{1}{2}(t_0+2t_1 -n(xt_0+2x_1))i+\frac{1}{2}(t_0+2t_2-n(xt_0+2x_2))j$$

$$+\frac{1}{2}(t_0+2t_3-n(xt_0+2x_3))k$$

إذا أمكننا اختيار الأعداد الصحيحة x_0,x_1,x_2,x_3 بحيث يكون

$$|t_0-nx_0|\leq\frac{1}{2}n,\ |t_0+2t_1-n(xt_0+2x_1)|\leq n,\ |t_0+2t_2-n(xt_0+2x_2)|\leq n,\ |t_0+2t_3-n(xt_0+2x_3)|\leq n$$

فينتج عن ذلك أن

$$N(a-cn)=\frac{(t_0-nx_0)^2}{4}+\frac{(t_0+2t_1-n(xt_0+2x_1))^2}{4}+\dots$$

$$\leqslant\frac{1}{16}n^2+\frac{1}{4}n^2+\frac{1}{4}n^2+\frac{1}{4}n^2<n^2=N(a)$$

وهي النتيجة المطلوبة. ولكننا الآن ندعي أنه يمكن دائما عمل ذلك:

(١) يوجد عدد صحيح x_0 بحيث $t_0=nx_0+r$ حيث $-\frac{1}{2}n\leqslant r\leqslant\frac{1}{2}n$. لهذا العدد x_0 يكون $|t_0-x_0n|=|r|\leqslant\frac{1}{2}n$.

(٢) يوجد عدد صحيح k بحيث $t_0+2t_1=kn+r$ و $0\leqslant r\leqslant n$. إذا كان $k-t_0$ عددًا زوجيًا فاجعل $2x_1=k-t_0$. حينئذ $t_0+2t_1=(2x_1+t_0)n+r$ و $|t_0+2t_1-(2x_1+t_0)n|=r<n$. من ناحية أخرى إذا كان $k-t_0$ فرديًا فاجعل $2x_1=k-t_0+1$. لذا

$$t_0+2t_1=(2x_1+t_0-1)n+r=(2x_1+t_0)n+r-n$$

وعليه

$$|t_0+2t_1-(2x_1+t_0)n|=|r-n|\leqslant n$$

لأن $0\leqslant r<n$. إذن يمكننا إيجاد عدد صحيح x_1 يحقق

$$|t_0+2t_1-(2x_1+t_0)n|\leqslant n$$

(٣) كما في الجزء الثاني يمكننا إيجاد عددين صحيحين x_2 و x_3 يحققان

$|t_0+2t_2-(2x_2+t_0)n|\leqslant n$ و $|t_0+2t_3-(2x_3+t_0)n|\leqslant n$

على الترتيب.

في الحالة الخاصة التي فيها a عنصر اختياري في H و b عدد صحيح موجب قد بيّنا أن التمهيدية صحيحة.

الآن نتحول إلى الحالة العامة التي فيها a و b عنصران اختياريان في H و $b\neq0$. باستخدام تمهيدية (٧-٤-٤) فإن $n=bb^*$ هو عدد صحيح موجب. لذا يوجد عنصران c و d_1 في H بحيث $ab^*=cn+d_1$ حيث $N(d_1)<N(n)$. لذا $N(ab^*-cn)<N(n)$ ولكن

$n=bb^*$ حينئذ نحصل على $N(ab^*-cbb^*)<N(n)$ فيكون $N((a-cb)b^*)<N(n)=N(bb^*)$.
من تمهيدية (٧-٤-٢) يصبح $N(a-cb)N(b^*)<N(b)N(b^*)$
ولكون $N(b^*)>0$ نحصل على $N(a-cb)<N(b)$. بجعل $d=a-cb$ يكون لدينا $a=cb+d$ بحيث $N(d)<N(b)$. إن هذا يكمل برهان التمهيدية.

كما في الحالة الإبدالية يمكننا أن نستنتج ما يلي من تمهيدية (٧-٤-٥).

تمهيدية (٧-٤-٦)

ليكن L مثاليًا أيسر في H. عندئذ يوجد عنصر u في L بحيث أن كل عنصر في L هو مضاعف أيسر لـ u. بعبارة أخرى، يوجد عنصر u في L بحيث لكل x في L يكون $x=ru$ حيث r في H.

البرهان

إذا كان $L=(0)$ فلا يوجد شيء نبرهنه، كل ما يجب أن نفعله هو أن نفرض أن $u=0$ لذا فيمكننا الفرض أن L يحوي عناصر لا تساوي الصفر. إن معيار العنصر غير الصفري هو عدد صحيح موجب (تمهيدية ٧-٤-٤) لذا يوجد عنصر $u\neq0$ في L بحيث يكون معياره أصغر ما يمكن بالنسبة إلى معايير العناصر غير الصفرية في L. إذا كان x في L فوفقًا لتمهيدية (٧-٤-٥)، $x=cu+d$ حيث $N(d)<N(u)$. ولكن d في L لأن كلًّا من x و u ومن ثم cu في L الذي هو مثالي أيسر. لذا $N(d)=0$ مما يجعل $d=0$. من هذا نستنتج أن $x=cu$.

قبل أن نتمكن من برهان مبرهنة المربعات الأربعة والتي هي غاية هذا البند يبقى علينا إثبات التمهيدية التالية.

تمهيدية (٧-٤-٧)

إذا كان a في H فإن a^{-1} في H إذا وفقط إذا كان $N(a)=1$.

البرهان

إذا كان كل من a و a^{-1} في H فإنه استنادا إلى تمهيدية (٧-٤-٤) يكون كل من N(a) و $N(a^{-1})$ عددًا صحيحًا موجبًا. ولكن $aa^{-1}=1$ ، لذا باستعمال تمهيدية (٧-٤-٢)، $N(a)N(a^{-1})=N(aa^{-1})=N(1)=1$. إن هذا يجعل $N(a)=1$.

من ناحية أخرى إذا كان a في H و $N(a)=1$ فإن $aa^*=N(a)=1$ وعليه يكون $a^{-1}=a^*$. ولكن من تمهيدية (٧-٤-٤) يكون a^* في H لأن a في H وعليه يصبح $a^{-1}=a^*$ في H أيضا.

إننا بذلك نكون قد حددنا ملامح كافية من بنية H لاستعمالها في دراسة بعض خواص الأعداد الصحيحة. الآن نبرهن المبرهنة التقليدية المشهورة للاجرانج.

مبرهنة (٧-٤-١)

يمكن كتابة كل عدد صحيح موجب كمجموع أربعة مربعات.

البرهان

إذا كان n عددا صحيحًا موجبًا فإننا ندعي في المبرهنة أن $n=x_0^2+x_1^2+x_2^2+x_3^2$ حيث x_0,x_1,x_2,x_3 أعداد صحيحة. لما كان كل عدد صحيح يتحلل إلى حاصل ضرب أعداد أولية، فإذا كان كل عدد أولي هو حاصل جمع لأربعة مربعات فعلى ضوء متطابقة لاجرانج (تمهيدية ٧-٤-٣) يصبح كل عدد صحيح موجب هو مجموع أربعة مربعات. بهذا نكون قد اختصرنا المسألة إلى اعتبار الأعداد الأولية n فقط. وبالطبع فإن العدد الأولي 2 يمكن كتابته على النحو $1^2+1^2+0^2+0^2$

دون المساس بعمومية البرهان يمكننا الفرض أن *n عدد أولي فردي*، والذي عادة يرمز له بالرمز p.

لنعتبر الرباعيات W_p على Z_p مجموعة الأعداد الصحيحة قياس p.

$$W_p=\{\alpha_0,+\alpha_1 i+\alpha_2 j+\alpha_3 k|\alpha_0,\alpha_1\alpha_2,\alpha_3\in Z_p\}$$

إن W_p حلقــة منتهية وبـالإضـافـة إلى ذلـك أنها غير إبـدالية لأن $ij=-ji\neq ji$ حيث $p\neq 2$. لذا من مبرهنة فدربرن لا يمكن لـ W_p أن تكون حلقة قسمة، واستنادًا لمسألة ١ في نهاية بند (٣ـ٥) يجب أن نحوي مثاليا أيسر لا يساوي كلا من (0) وW_p.

ولـكــن حينئــذ لا يمكــن للمثـالي ثنائي الجـانب V في H والـمعــرف بـ $V=\{x_0\zeta+x_1i+x_2j+x_3k|p$ يقسم كلا من $x_0,x_1,x_2,x_3\}$ أن يكــون مثــالــيًا أيسرًا أعـظميا في H لأن H/V يماثل W_p. (برهن على ذلك) (لو كان V مثاليا أيسر أعظميا في H فحينئذ H/V ومن ثم W_p لا يمكن أن تحوي مثاليات يسرى عدا (0) و H/V).

لذا يوجـد مثـالي أيسر L في H يحقق: $L\neq H$ ، $L\neq V$ و $L\supset V$. وفقا لتمهيدية (٧ـ٤ـ٦) يوجد عنصر u في L بحيث أن كل عنصر في L هو مضاعف أيسر لـ u. لما كان $p\in V$ فإن $p\in L$ وعليه $p=cu$ لعنصر c في H. وحيث إن $u\notin V$ لا يمكن أن يوجد معكوس لـ c في H لأنه حينئذ $u=c^{-1}p$ سيكون في V. لذا $N(c)>1$ استنادا لتمهيدية (٧ـ٤ـ٧).
لما كان $L\neq H$ فلا يوجد معكوس لـ u في H مما يجعل $N(u)>1$. ولكون $p=cu$ فإن

$$p^2=N(p)=N(cu)=N(c)N(u)$$

ولكن $N(c)$ و $N(u)$ عددان صحيحان لأن كلا من c و u في H ، كما أن كلا منهما أكبر من ١ ، وكل منهما يقسم p^2. حينئذ لابد وأن يكون $N(c)=N(u)=p$.

لما كان $u\in H$ ، $u=m_0\zeta+m_1i+m_2j+m_3k$ حيث m_0,m_1,m_2,m_3 أعداد صحيحة لذا

$$2u=2m_0\zeta+2m_1i+2m_2j+2m_3k=(m_0+m_0i+m_0j+m_0k)+2m_1i+2m_2j+2m_3k$$
$$=m_0+(2m_1+m_0)i+(2m_2+m_0)j+(2m_3+m_0)k$$

إذن $N(2u)=m_0^2+(2m_1+m_0)^2+(2m_2+m_0)^2+(2m_3+m_0)^2$. ولكن $N(2u)=N(2)N(u)=4p$ لأن $N(u)=p,\ N(2)=4$. لقد بيّنا أن $4p=m_0^2+(2m_1+m_0)^2+(2m_2+m_0)^2+(2m_3+m_0)^2$.
إننا على وشك أن ننتهي من البرهان.

كي ننــهي البرهـان نقـدم إحـدى الحيل القـديـمـة لـ أويـلـر: إذا كان $2a=x_0^2+x_1^2+x_2^2+x_3^2$ حيث x_0,x_1,x_2,x_3 أعـداد صحيحة فإن $a=y_0^2+y_1^2+y_2^2+y_3^2$

لأعداد صحيحة y_0, y_1, y_2, y_3. كي نرى هذا لاحظ أنه لكون $2a$ عددًا زوجيًا فإن الأعداد $x_i, 0 \leqslant i \leqslant 3$ إما تكون كلها زوجية أو كلها فردية أو اثنان منهما فرديين واثنان زوجيين. في جميع الأحوال يمكننا إعادة ترقيم الـ $x_i, 0 \leqslant i \leqslant 3$ وتجميعها في أزواج بحيث

$$y_0 = \frac{x_0 + x_1}{2},\ y_1 = \frac{x_0 - x_1}{2},\ y_2 = \frac{x_2 + x_3}{2},\ y_3 = \frac{x_2 - x_3}{2}$$

كلها أعداد صحيحة. ولكن

$$y_0{}^2 + y_1{}^2 + y_2{}^2 + y_3{}^2 = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2$$

$$= \frac{1}{2}(x_0{}^2 + x_1{}^2 + x_2{}^2 + x_3{}^2)$$

$$= \frac{1}{2}(2a) = a$$

لما كان $4p$ يساوي مجموع أربعة مربعات، وفقا للملاحظة أعلاه يكون $2p$ كذلك. ولكون $2p$ يساوي مجموع أربعة مربعات فإن p يكون كذلك أيضا. لذا $p = a_0{}^2 + a_1{}^2 + a_2{}^2 + a_3{}^2$ حيث a_0, a_1, a_2, a_2 أعداد صحيحة، وبهذا نكون قد برهنا على مبرهنة لاجرانج.

إن هذه المبرهنة تعتبر نقطة البداية لمجال بحث واسع في نظرية الأعداد والذي يسمى **مسألة وورينج** (Waring). إن هذه المسألة تسأل عما إذا كان عدد صحيح يساوي مجموع عدد معيّن من الأعداد مرفوعة للقوة k. على سبيل المثال يمكن برهان أن كل عدد صحيح هو حاصل جمع تسعة مكعبات ومجموع تسعة عشر عدد مرفوع للقوة الرابعة. . . الخ. لقد أثبت الرياضي العظيم **هلبرت** (Hilbert) أن لمسألة وورينج جواب إيجابي.

مسائل

١ - برهن تمهيدية (٧-٤-٤).

٢ - أوجد جميع العناصر α في Q_0 بحيث أن α^{-1} في Q_0 أيضا.

٣ - برهن على أنه يوجد بالضبط 24 عنصرًا a في H بحيث أن a^{-1} في H أيضا. حدد جميع هذه العناصر.

٤ - أعط مثالاً لعنصرين a و b في Q_0 ، $b\neq 0$ بحيث أنه من المستحيل إيجاد عنصرين c و d في Q_0 يحققان $a=cb+d$ حيث $N(d)<N(b)$.

٥ - أثبت أنه إذا كان a في H فيوجد عددان صحيحان α و β بحيث $a^2+\alpha a+\beta=0$.

٦ - أثبت أنه يوجد عدد صحيح موجب لا يمكن كتابته كحاصل جمع ثلاثة مربعات.

*٧ - بيّن أنه يوجد عدد غير منته من الأعداد الصحيحة الموجبة التي لا يمكن كتابتها كحاصل جمع ثلاثة مربعات.

قراءة إضافية

لغرض دراسة أعمق للحقول المنتهية انظر:

Albert, A. A. *Fundamental Concepts of Higher Algebra.* Chicago: University of Chicago Press, 1956.

● لغرض الاطلاع على عدة براهين لمبرهنة المربعات الأربعة ولدراسة لمسألة وورينج انظر:

Hardy, G.H., and Wright, E.M. *An Introduction to the Theory of Numbers,* 4th Ed. New York: Oxford University Press, 1960.

● لغرض الاطلاع على برهان آخر لمبرهنة قدربرن انظر :

Artin, E. "Über einen satz von Hern J. H. M. Wedderburn". *Abhandlungen, Hamburg Mathematisches Seminar.* **5** (1928), 245-50.

ثبت المصطلحات

أ

إبدالية	Commutative
آبلية	Abelian
اتحاد	Union
أثر	Trace
إدخال	Embedding
ارتباط خطي	Linearly dependence
أساس	Basis
ثنوي	Dual basis
متعامد معاير	Orthonormal basis
استقطار	Diagonalization
استقلال خطي	Linearly independence
إسقاط	Projection
أعداد جاوس	Gaussian integers
جبرية	Algebraic numbers
جبرية صحيحة	Algebraic integers
صحيحة أولية نسبيًا	Relatively prime integers
اقتصار تطبيق	Restriction of mapping

Eucledian	إقليدي
Extension	امتداد
Simple extension	بسيط
Algebraic extension	جبري
Separable extension	قابل للفصل
Finite extension	منته
Normal extension	ناظمي
Reflexive	إنعكاسية
Prime	أولي

ب

Quadratic residue	باقي تربيعي
Primitive	بدائي
Dimension	بُعد
Structure	بنية

ت

Permutation	تبديل
Even permutation	زوجي
Odd permutation	فردي
Trisecting an angle	تثليث الزاوية
Partition	تجزئة
Associative	تجميعي (دامج)
Linear transformation	تحويل خطي
Singular linear transformation	شاذ
Non negative linear transformation	غير سالب
Idempotent linear transformation	متساوي القوى
Nilpotent linear transformation	معدوم القوى

Regular linear transformation	منتظم	
Positive definite linear transformation	موجب بالتحديد	
Normal linear transformation	ناظمي	
Hermition linear transformation	هرميتي	
Unitary linear transformation	واحدي	
Conjugation		ترافق
Composition of mapping	تطبيقات	تركيب
Linear combination	خطي	
Transcendence		تسام
Homomorphism		تشاكل
Homomorphism of rings	الحلقات	
Homomorphism of groups	الزمر	
Homomorphism of modules	الفضاءات الحلقية	
Homomorphism of vector spaces	فضاءات المتجهات	
Congruence		تطابق
Congruence module a subgroup	قياس زمرة جزئية	
Congruence module n	قياس n	
Mapping		تطبيق
One-to-one mapping	أحادي	
Onto mapping	غامر	
Perpendicularity		تعامد
Transitivity		تعدي
Decomposition		تفريق
Cyclic decomposition	الدورة	
Spectral resolution	طيفي	
One-to-one correspondence		تقابل

تقسيم	Division
تكرار	Multiplicity
الجذور	Multiplicity of roots
الجذور المميزة	Multiplicity of characteristic roots
تماثل	Isomorphism
الحلقات	Isomorphism of rings
ذاتي	Automorphism
خارجي	Outer automorphism
داخلي	Inner automorphism
الزمر	Isomorphism of groups
الفضاءات الحلقية	Isomorphism of modules spaces
فضاءات المتجهات	Isomorphism of vector spaces
تمثيل	Representation
تبديلي	Permutation representation
تبديلي ثان	Second permutation representation
تناظر	Symmetric
توليد خطي	Linear span

ث

ثنوي	Dual
ثانٍ	Second dual

ج

جبر	Algebra
بوليني	Boolean algebra
التحويلات الخطية	Algebra of linear transformations
خطي	Linear algebra
القسمة الجبري	Algebraic division algebra

Matrix algebra	المصفوفات
Algebraic	جبري
Algebraic of degree n	من الدرجة n
Root	جذر
Primitive root	بدائي
Primitive root of prime number	للعدد الأولي
Primitive root of *n*th root of unity	للواحد من رتبة n
Root of polynomial	كثيرة الحدود
Radical of an ideal	المثالي
Multiple of root	مكرر
Characteristic root	مميز
Sum	جمع
Direct sum	مباشر
External direct sum	خارجي
Internal direct sum	داخلي

ح

Field	حقل
Splitting field	انشطار
Skew-field	تخالفي
Field of quotients	خوارج القسمة
Perfect field	كامل
Isomorphic rings	حلقات متماثلة
Ring	حلقة
Commutative ring	إبدالية
Eucledian ring	إقليدية
Ring with unity	بعنصر وحدة

بولينية	Boolean ring
تامة	Integral domain
تجميعية	Associative ring
التحويلات الخطية	Ring of linear transformations
خارجة	Quotient ring
غير تجميعية	Non associative ring
قسمة	Division ring
كثيرات الحدود	Ring of Polynomials
في n متغير	Ring of polynomials in n variable
المصفوفات من نوع 2×2	Ring of 2×2 matrices

خ

خارج	Quotient
خطي	Linear
خوارزم	Algorithm
إقليدي	Eucledian algorithm
القسمة	Division algorithm
القسمة الأيسر	Left division algorithm

د

دالِّي	Functional
خطي	Linear functional
دالة فاي (لأويلر)	Euler phi function
درجة	Degree
الامتداد	Degree of extension
كثيرة الحدود	Degree of polynomial
دليل	Index
انعدام القوى	Index of nilpotence

دوال ابتدائية	Elementary functions
نسبية	Rational functions
نسبية متناظرة	Symmetric rational functions
متناظرة	Symmetric functions
دور	Period
العنصر	Period of an element
دورة	Cycle
دوري	Cyclic

ر

رباعيات	Quaternions
حقيقية	Real quaternions
رتبة	Order
الزمرة	Order of a group
العنصر	Order of an elment

ز

زمر متماثلة	Isomorphic groups
جزئية مترافقة	Conjugate subgroups
زمرة	Group
إبدالية	Commutative group
آبلية	Abelian group
بسيطة	Simple group
التبديلات	Permutation group
التماثلات الذاتية الخارجية	Group of outer automorphism
الداخلية	Group of inner automorphism
التناظر من الدرجة n	Symmetric group of degree n
جالوا	Galios group

زمرة جزئية	Subgroup
تافهة	Trivial subgroup
دورية	Cyclic subgroup
غير تافهة	Non trivial subgroup
مميزة	Characteristic subgroup
ناظمية	Normal subgroup
خارجة	Quotient group
دورية	Cyclic subgroup
زوجية	Dihedral group
سيلو الجزئية من نوع p	p-Sylow subgroup
قابلة للحل	Solvable group
المبدلات الجزئية	Commutator subgroup
الجزئية العليا	Higher commutator subgroup
متناوبة من الدرجة n	Alternating group of degree n
معدومة القوى	Nilpotent group
منتهية	Finite group
وحدات الرباعيات	Group quaternions units

ش

شاذ	Singular
شريك	Associate

ص

صف المصفوفة	Row of matrix
صورة	Image
معكوسة	Inverse image
صيغة تربيعية	Quadratic form
حقيقية	Real quadratic form
جوردان القانونية	Jordan canonical form

Canonical form	صورة قانونية
Rational canonical form	نسبية
Triangular form	مثلثة

ض

Product of mappings	ضرب تطبيقات
Inner product	داخلي
Cartesian product	ديكارتي
Scalar product	قياسي
Direct product	مباشر
External direct product	خارجي
Internal direct product	داخلي

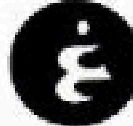
ط

Gram-Schmidt orthogonolization process	طريقة جرام ـ شميدت للتعامد

ع

Cofactor	عامل مرافق
Prime number	عدد أولي
Algebraic number	جبري
Algebraic integer	صحيح
Constructable number	قابل للإنشاء
Transcendental number	متسامٍ
Relation	علاقة
Reflexive relation	انعكاسية
Equivalence relation	تكافؤ
Binary relation	ثنائية
Transitive relation	متعدية

متناظرة	Symmetric relation
عمود مصفوفة	Column of matrix
عنصر أولي	Prime element
جبري	Algebraic element
غير مختزل	Irreducible element
محايد	Identity element



غامر (شامل)	Onto
غير إبدالي	Non commutative
تجميعي	Non associative
متغير	Invariant
مختزل	Irreducible
منته	Infinite



فرق تناظري	Symmetric difference
فصل ترافق	Conjugacy class
تشابه	Similarity class
تطابق	Congruence class
تكافؤ	Equivalence class
فضاءات متجهات متماثلة	Isomorphic vector spaces
فضاء ثنوي	Dual space
جزئي (فضاء متجهات جزئي)	Subspace
دوري	Cyclic subspace
غير متغير	Invariant subspace
فضاء حلقي	Module
جزئي	Submodule

Quotient module	خارج
Cyclic module	دوري
Irreducible module	غير مختزل
Finitely generated module	منته التوليد
Unital module	واحدي
Inner product space	فضاء الضرب الداخلي
Vector space	فضاء متجهات
Subspace	جزئي
Real vector space	حقيقي
Quotient vector space	خارج

ق

Constructable	قابل للإنشاء
Solvable	للحل
Separable	للفصل
Solvability by radical	قابلية الحل باستخلاص الجذور
Divisibility	القسمة
Divisor	قاسم
Zero divisor	للصفر
Greatest common divisor	مشترك أعظم
Jordan block	قالب جوردان
Commutative law	قانون الإبدال
Associative law	التجميع (الدمج)
Adjoint	قرين
Self adjoint	ذاتي
Quaternion adjoint	رباعي
Hermitian adjoint	هرميتي

قسمة	Division
جبرية	Algebraic division
قواسم ابتدائية	Elementary divisors
قوانين الاختزال	Cancellation laws
التوزيع	Distribution laws
قياسي	Scalar
قيمة واقعية	Eigenvalue

ك

كثيرة حدود	Polynomial
دنيا	Minimal polynomial
بدائية	Primitive polynomial
دورية	Cyclotomic polynomial
غير مختزلة	Irreducible polynomial
متناظرة	Symmetric polynomial
مميزة	Characteristic polynomial

م

مبدأ توزيع الأماكن	Pigeonhole principle
مبدل	Commutator
مبرهنة	Theorem
متباينة	Inequality
متسع منتظم	Regular 9-gon
متجه مميز	Characteristic vector
متممة	Complement
متمم عمودي	Orthogonal complement
مثالي	Ideal
أعظمي	Maximal ideal
أولي	Prime ideal

Left ideal	أيسر
Right ideal	أيمن
Principal ideal	رئيس
Disjoint sets	مجموعات منفصلة
Set	مجموعة
Set of integrs moduls n	الأعداد الصحيحة قياس n
Irreducible set of linear transformations	التحويلات الخطية غير المختزلة
Decomposable set of linear transformations	التحويلات الخطية القابلة للتفريق
Subset	جزئية
Proper subset	فعلية
Empty set	خالية
Index set	الدليل
Infinite set	غير منتهية
Difference set	الفرق
Orthonormal set	متعامدة معايرة
Coset	مشاركة
Double coset	مزدوجة
Left coset	يسرى
Right coset	يمنى
Content of polynomial	محتوى كثيرة حدود
Determinant	محدّدة
Pentagon	مخمس
Range	مدى
Conjugate	مرافق
Rank	مرتبة

Rank of linear transformation	مرتبة التحويل الخطي
Rank of module	الفضاء الحلقي
Rank of matrix	المصفوفة
Center of a group	مركز الزمرة
Septagon	مسبع
Hexagon	مسدس
Axiom of choice	مسلمة الاختيار
Similar	مشابه
Derivative	مشتقة
Matrix	مصفوفة
Permutation matrix	تبديلية
Matrix of linear transformation	تحويل خطي
Zero matrix	صفرية
Diagonal matrix	قطرية
Scalar matrix	قياسية
Orthogonal matrix	متعامدة
Symmetric matrix	متناظرة
Skew symmetric matrix	تخالفيا
Real symmetric matrix	حقيقية
Triangular matrix	مثلثة
Companion matrix	مصاحبة
n×n matrix	من نوع n×n
Matrix unit	الوحدة
Hermitian matrix	هرميتية
Least common multiple	مضاعف مشترك أصغر
Regular 15-gon	مضلع منتظم ذو الخمسة عشر ضلعا

Regular 17-gon	مضلع منتظم ذو السبعة عشر ضلعا
Congruent	مطابــق
Homogeneous linear equation	معادلات خطية متجانسة
Secular equation	معادلة عامة
Class equation	الفصول
coefficients	معاملات
Inverse	معكــوس
Left inverse	أيسر
Right inverse	أيمــن
Inverse of mapping	تطبيــق
Inverse of an element	عنصر
Criterion	معيار
Annihilator	مفني
Annihilator of subspace	الفضاء الجزئي
Modulus	مقياس
Centralizer	ممركز
Centralizer of subgroup	الزمرة الجزئية
Centralizer of an element	العنصر
Characteristic	مميز
Characteristic of integral domain	الحلقة التامة
Zero characteristic	صفري
Finite	منته
Finite dimensional	البعد
Finite characteristic	المميز
Normalizer	منظم (معاير)
Mutually disjoint	منفصلة تبادليا

منقول	Transpose
موجب بالتحديد	Positive definite
مولد	Generator
خطي	Linear span

ن

نظام ضربي	Multiplicative system
معادلات خطية	System of linear equations
نواة	Kernel

و

واحدي	Unital
وحدة	Unit

كشاف الموضوعات

الدكتور/ فوزي بن أحمد الصالح الذكير

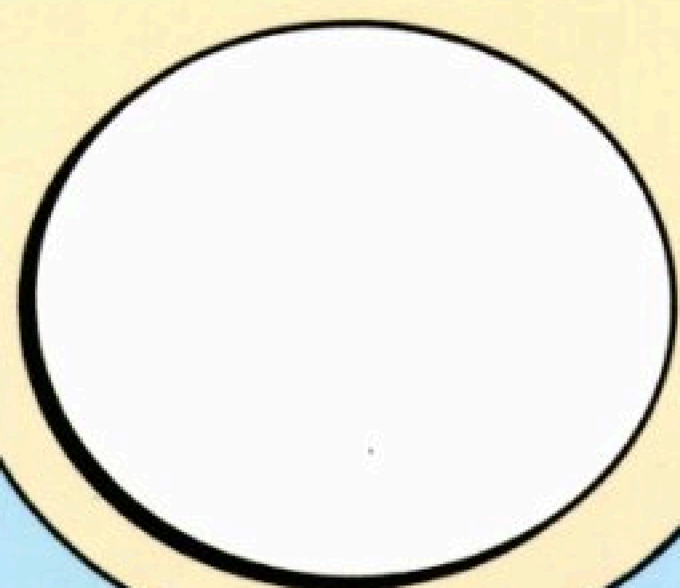
أستاذ مشارك في قسم الرياضيات بكلية العلوم، جامعة الملك سعود. حصل على درجة الدكتوراه في علم الرياضيات من جامعة كاليفورنيا في لوس أنجلوس بالولايات المتحدة الأمريكية عام ١٤٠١هـ (١٩٨١م). عمل في عدة لجان في القسم وفي كلية العلوم (منها مجلس كلية العلوم)، ثم أصبح رئيساً لقسم الرياضيات في الفترة من ١٤١٢هـ إلى ١٤١٤هـ (١٩٩٢م - ١٩٩٤م). ويسند إليه حالياً منصب رئيس الجمعية السعودية للعلوم الرياضية.

قام بنشر عدة أبحاث في نظرية الزمر، المجموعات المرتبة جزئياً، نظرية المجموعات المشوشة بالإضافة إلى تطبيقات الرياضيات في مجال الاتصالات. شارك في تأليف كتاب في نظرية الأعداد، كما أنه شارك في تأليف كتب دراسية في علم الرياضيات لتدريسها في المرحلة الثانوية، بالإضافة إلى المشاركة في ترجمة بعض المراجع العلمية في علم الرياضيات.

الدكتور/ علي بن عبدالله بن صالح السحيباني

يعمل حالياً أستاذاً مشاركاً في قسم الرياضيات بكلية العلوم، جامعة الملك سعود. حصل على درجة الدكتوراه في علم الرياضيات من جامعة برمنجهام في بريطانيا عام ١٣٩٩هـ (١٩٧٩م). عمل في عدة لجان في القسم، وأصبح رئيساً للقسم في الفترة من ١٤٠٣هـ إلى ١٤٠٥هـ.

قام بنشر عدة أبحاث في الجبر، وأسهم في تأليف عدة كتب دراسية في الرياضيات لتدريسها في الكليات المتوسطة، كما شارك في ترجمة بعض المراجع العلمية في علم الرياضيات.



ردمك : ٩٩٦٠-٣٧-٨٦-٠

ISBN:9960-37-86-0